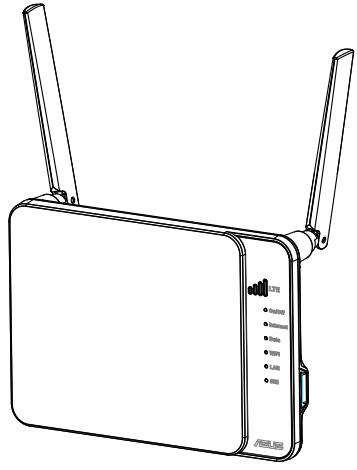
Manual de usuario

4G-N12

Enrutador/Módem LTE inalámbrico N300



IN SEARCH OF INCREDIBLE

S9553
Primera edición
De noviembre 2014

Copyright © 2014 ASUSTeK Computer Inc. Todos los derechos reservados.

Se prohíbe la reproducción, transmisión, transcripción, almacenamiento en un sistema de recuperación o traducción a cualquier idioma de este manual, íntegra o parcialmente, incluidos los productos y el software que en él se describen, de ninguna forma ni a través de ningún medio, a excepción de que tales actividades sean llevadas a cabo por el comprador con fines de conservación, sin autorización expresa por escrito de ASUSTeK Computer Inc. ("ASUS").

La garantía y los servicios de reparación vinculados al producto no serán de aplicación si: (1) el producto ha sido reparado, modificado o alterado, a excepción de que tal reparación, modificación o alteración haya sido autorizada por escrito por ASUS; o (2) no sea posible determinar el número de serie del producto o aquél no se encuentre presente.

ASUS PROPORCIONA ESTE MANUAL "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPRESAS NI IMPLÍCITAS, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS O CONDICIONES DE COMERCIABILIDAD O AJUSTE A UNA FINALIDAD EN PARTICULAR. NI ASUS, NI SUS DIRECTORES, RESPONSABLES, EMPLEADOS O AGENTES SERÁN RESPONSABLES DE NINGÚN DAÑO INDIRECTO, ESPECIAL, ACCIDENTAL O CONSECUENTE (INCLUIDOS AQUÉLLOS DERIVADOS DE PÉRDIDAS DE BENEFICIOS, PÉRDIDAS DE OPORTUNIDADES COMERCIALES, IMPOSIBILIDAD DE USAR EL EQUIPO, PÉRDIDAS DE DATOS, INTERRUPCIONES DE LA ACTIVIDAD COMERCIAL Y OTROS PERJUICIOS DE CARÁCTER SIMILAR), AÚN CUANDO ASUS HAYA SIDO ADVERTIDA DE LA POSIBILIDAD DE QUE TALES DAÑOS TENGAN LUGAR COMO RESULTADO DE ALGÚN DEFECTO O ERROR EN ESTE MANUAL O EN EL PRODUCTO.

LAS ESPECIFICACIONES Y LA INFORMACIÓN QUE CONTIENE ESTE MANUAL SE PONEN A DISPOSICIÓN DEL PROPIETARIO CON FINES EXCLUSIVAMENTE INFORMATIVOS; AMBAS SE ENCUENTRAN SUJETAS A CAMBIOS EN CUALQUIER MOMENTO SIN AVISO PREVIO Y NO DEBEN CONSIDERARSE UN COMPROMISO EMPRENDIDO POR ASUS. ASUS NO ASUME RESPONSABILIDAD U OBLIGACIÓN ALGUNA EN RELACIÓN CON AQUELLOS ERRORES O IMPRECISIONES QUE ESTE MANUAL PUDIERA CONTENER, INCLUIDOS LOS PRODUCTOS Y EL SOFTWARE QUE EN ÉL SE DESCRIBEN.

Los nombres de productos y empresas que aparecen en este manual podrían ser o no marcas comerciales registradas o estar vinculados a derechos de autor en posesión de sus respectivas empresas propietarias; su uso se lleva a cabo exclusivamente con fines de identificación y explicación y en beneficio del propietario del producto, sin intención alguna de infringir los derechos indicados.

Contenidos

1 Conociendo su router inalámbrico

1.1 ¡Bienvenido! 5

1.2 Contenido del paquete 5

1.3 El router inalámbrico 6

1.4 Ubicar el router 8

1.5 Requisitos de configuración 9

1.6 Configuración del router 10

2 Introducción

2.1 Inicio de sesión en la interfaz gráfica del usuario web 12

2.2 Función Configuración rápida de Internet (QIS, Quick Internet Setup) con detección automática 13

3 Definir la configuración general

3.1 Utilizar el mapa de red 16

3.2 SMS 16

3.2.1 Nuevo SMS 17

3.2.2 Bandeja de entrada 18

3.2.3 Borradores 18

3.2.4 Libreta de teléfonos 18

4 Definición de la configuración avanzada

4.1 Inalámbrico 19

4.1.1 General 19

4.1.2 Configuración de RADIUS 22

4.1.3 Filtro MAC inalámbrico 23

4.1.4 WPS (Wi-Fi Protected Setup, es decir, configuración protegida Wi-Fi) 24

4.2 LAN 26

4.2.1 Configuración LAN 26

4.2.2 Lista de clientes DHCP 28

Contenidos

4.3 WAN 28
4.3.1 Conexión a Internet 28
4.3.2 Estado de la conexión móvil 32
4.3.3 Búsqueda de conexión móvil 34
4.3.4 UPnP 35
4.3.5 Servidores virtuales/Reenvío de puertos 36
4.3.6 DMZ 37
4.3.7 DDNS 39
4.4 Firewall 40
4.4.1 General 40
4.4.2 Filtro MAC 41
4.4.3 Detección de intrusiones 42
4.4.4 Control de acceso 43
4.4.5 Filtro de direcciones URL 45
4.4.6 Regla de programación 46
4.5 Administración 47
4.5.1 Sistema 47
4.5.2 Actualización del firmware 48
4.5.3 Restaurar / Guardar / Enviar configuración 48
4.6 Registro del sistema 49
4.7 Herramientas de red 50
4.7.1 Ping 50
4.7.2 Traceroute 51
4.7.3 Captura WAN 52

5 Preguntas más frecuentes (P+F)

Apéndices

Notas 56
Información de contacto con ASUS 69
Información telefónica internacional acerca de redes 70

1 Conociendo su router inalámbrico

1.1 ¡Bienvenido!

¡Gracias por adquirir un enrutador LTE inalámbrico 4G-N12 de ASUS!

El enrutador LTE inalámbrico 4G-N12 de ASUS incluye un módulo de red 4G, que le permite insertar una tarjeta SIM/USIM para acceder a su LTE 4G o conexión de red 3G, así como compartirlos, a través de una red inalámbrica segura o de cualquiera de los cuatro puertos Ethernet. Ofrece una velocidad de descarga y carga de 100 y 50 Mbps, respectivamente, que proporciona acceso a Internet rápido, streaming multimedia sin problemas o transferencia de datos sencilla.

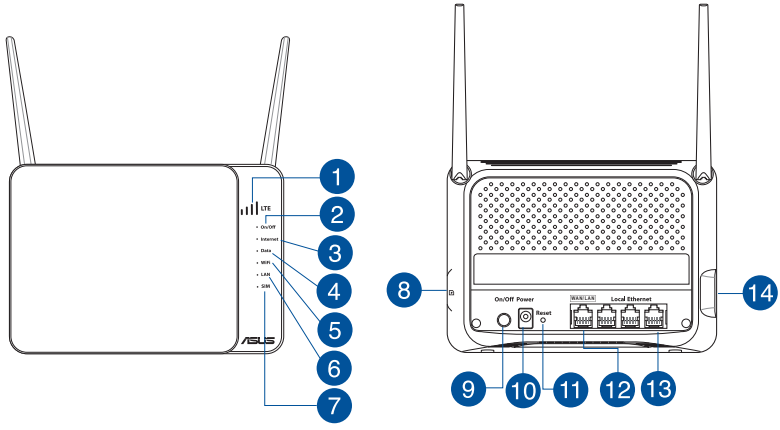
1.2 Contenido del paquete

- ☑ Router inalámbrico 4G-N12
- ☑ Adaptador de alimentación
- ☑ Cable de red (RJ-45)
- ☑ Guía de inicio rápido

NOTAS:

- Si cualquiera de los artículos falta o se encuentra dañado, póngase en contacto con ASUS para realizar preguntas técnicas u obtener soporte técnico. Consulte la lista de números de teléfono de soporte técnico de ASUS que se encuentra en la parte posterior de esta guía.
- Conserve el material de embalaje original por si necesitara hacer uso de la garantía para realizar reparaciones o sustituciones.

1.3 El router inalámbrico



1 LED 1~4 LAN de LTE intensidad de señal

1 LED iluminado: señal muy débil;
2 LED iluminados: señal débil;
3 LED iluminados: señal normal;
4 LED iluminados: señal intensa.

2 LED de encendido y apagado

Apagado: no hay alimentación.
Encendido: dispositivo preparado.

3 LED de Internet

Apagado: no hay conexión LTE.
Intermitente: se está estableciendo una conexión WAN LTE/Ethernet.
Encendido: hay una conexión WAN LTE/Ethernet adecuada.

4 LED de datos (tráfico WAN LTE/Ethernet)

Apagado: no hay actividad de datos.
Encendido: conexión de datos preparada.

5 LED Wi-Fi

Apagado: no hay señal de 2,4 GHz.
Encendido: sistema inalámbrico preparado.

6 LAN LED

Apagado: no hay alimentación o no hay conexión física.
Encendido: hay conexión física con una red de área local (LAN).

7	**LED de tarjeta USIM** **Apagado**: no hay tarjeta USIM instalada. **Encendido**: hay tarjeta USIM instalada correctamente.
8	**Ranura para tarjetas USIM** Instale una tarjeta USIM en esta ranura para establecer una conexión LTE WAN.
9	**Botón de encendido** Presione este botón para encender o apagar el sistema.
10	**Puerto de alimentación (entrada de CC)** Inserte el adaptador de CA integrado en este puerto y conecte el router a una toma de corriente.
11	**Botón Restablecer** Presione este botón durante 5 segundos como mínimo para restablecer o restaurar la configuración predeterminada de fábrica del sistema.
12	**Puerto WAN/LAN** Mediante un cable Ethernet, conecte el módem a un puerto WAN/LAN del enrutador inalámbrico.
13	**Puertos LAN** Connect network cables into these ports to establish LAN connection.
14	**WPS button** This button launches the WPS Wizard.

NOTAS:

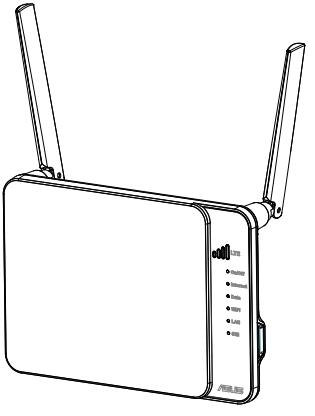
- Utilice únicamente el cargador incluido con el paquete. Si usa otros adaptadores, el dispositivo puede resultar dañado.
- Asegúrese de insertar la tarjeta SIM en la ranura para tarjetas antes de encender el enrutador.
- **Especificaciones:**

Adaptador de alimentación de CC	**Salida de CC:** +12 V con una corriente máxima de 1A		
Temperatura de funcionamiento	0~40°C	**Almacenamiento**	0~70°C
Humedad de funcionamiento	50~90%	**Almacenamiento**	20~90%

1.4 Ubicar el router

Para conseguir la mejor transmisión de señal inalámbrica entre el router inalámbrico y los dispositivos de red conectados a él, asegúrese de:

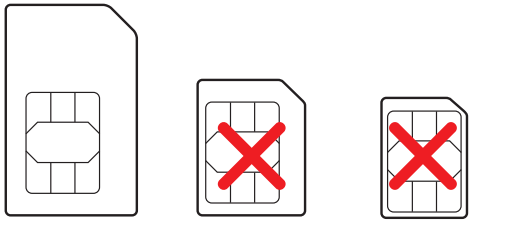
- Coloque el enrutador LTE inalámbrico cerca de una ventana para recibir la mejor calidad de señal LTE y conseguir un rendimiento máximo en el enlace de subida con la estación base LTE.
- Mantenga el dispositivo alejado de obstáculos metálicos y de la luz solar directa.
- No coloque el enrutador LTE inalámbrico en un entorno con polvo o humedad.
- Mantenga el producto alejado de dispositivos WiFi de 802.11g o 20 MHz, equipos periféricos de 2,4 GHz, dispositivos Bluetooth, teléfonos inalámbricos, transformadores, motores de alto rendimiento, luces fluorescentes, hornos microondas, frigoríficos y otros equipos industriales para evitar interferencias o pérdidas de señal.
- Actualícese siempre a la versión be firmware más reciente. Visite el sitio Web de ASUS en **http://www.asus.com** para obtener las actualizaciones de firmware más recientes.
- Para garantizar la mejor señal inalámbrica, oriente las tres antenas desmontables tal y como se muestra en el dibujo siguiente.



1.5 Requisitos de configuración

Para configurar la red inalámbrica, es necesario cumplir los siguientes requisitos:

- Una tarjeta mini-SIM/USIM con suscripción WCDMA y LTE



Mini SIM card **Micro SIM card** **Nano SIM card**

NOTA: Una tarjeta SIM/USIM estándar es una tarjeta mini-SIM estándar.

¡**IMPORTANTE**! Asegúrese de que la tarjeta SIM/USIM está suscrita a los servicios WCDMA y LTE. Póngase en contacto con su proveedor de servicio móvil para obtener información acerca de estos servicios.

¡PRECAUCIÓN! Utilice solamente una tarjeta SIM/USIM estándar en su enrutador. Si utiliza una tarjeta SIM con una forma diferente, como por ejemplo una tarjeta micro-SIM o nano-SIM, puede dañar el enrutador.

- Un módem de cable/ADSL con suscripción a Internet
- Un equipo con un puerto RJ-45 (LAN) Ethernet (10Base-T/100Base-TX) o un dispositivo Wi-Fi con una interfaz inalámbrica 802.11 b/g/n de 2,4 GHz
- Explorador web, como por ejemplo Internet Explorer, Firefox, Safari o Google Chrome

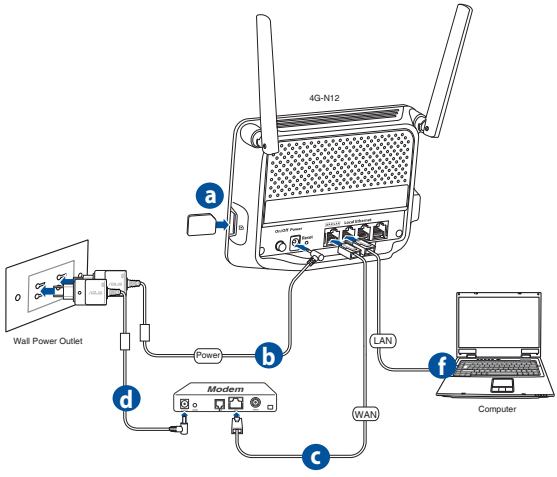
NOTAS:

- Si el equipo no cuenta con funcionalidad inalámbrica integrada, puede instalar un adaptador WLAN IEEE 802.11a/b/g/n en él para conectarse a la red.
- No enchufe un conector telefónico al puerto RJ-45. Si no sigue esta recomendación, el enrutador LTE inalámbrico podría resultar dañado.
- Los cables Ethernet RJ-45 que se utilizarán para conectar dispositivos de red no deben tener más de 100 metros.

1.6 Configuración del router

¡ADVERTENCIA!

- No instale el enrutador LTE inalámbrico durante una tormenta eléctrica. Existe riesgo potencial de que se produzca una descarga eléctrica a consecuencia de los rayos.
- No intente desmontar ni volver a montar este dispositivo. La manipulación del enrutador LTE inalámbrico puede anular esta garantía.
- Cuando instale o limpie el dispositivo, asegúrese de desenchufar el cable de alimentación del enrutador LTE inalámbrico.
- Para evitar descargas eléctricas, mantenga las manos secas cuando manipule el enrutador LTE inalámbrico.



a. Inserte la tarjeta SIM/USIM en la ranura para tarjetas USIM.

b. Inserte el adaptador de CA del enrutador en el puerto ENTRADA DE CC y enchúfelo a una toma de corriente eléctrica.

c. Mediante un cable de red, conecte el módem a un puerto WAN/LAN del enrutador inalámbrico.

d. Inserte el adaptador de CA del módem en el puerto ENTRADA DE CC y enchúfelo a una toma de corriente eléctrica.

e. Encienda el enrutador.

f. Mediante el cable de red incluido, conecte el equipo al puerto LAN del enrutador.

g. Para conectarse manualmente a una red inalámbrica:

1. Habilite la función Wi-Fi en el cliente inalámbrico para que busque automáticamente las redes inalámbricas.
2. Seleccione la red inalámbrica llamada "ASUS", que es el nombre de red inalámbrico predeterminado (SSID) de los enrutadores inalámbricos de ASUS.
3. Cuando se le pida, escriba la contraseña predeterminada del enrutador, que puede encontrar en la pegatina situada en la parte posterior.

2 Introducción

2.1 Inicio de sesión en la interfaz gráfica del usuario web

El router inalámbrico de ASUS incluye una intuitiva interfaz gráfica del usuario web (GUI, Graphics User Interface) que permite configurar fácilmente sus distintas funciones mediante un explorador web, como por ejemplo Internet Explorer, Firefox, Safari o Google Chrome.

NOTA: Las características pueden variar en función de las diferentes versiones de firmware.

Para iniciar sesión en la interfaz gráfica del usuario web:

1. En su explorador web (Internet Explorer, Firefox, Safari o Google Chrome) inserte manualmente la dirección IP predeterminada del router inalámbrico: **192.168.1.1** o escriba http://router.asus.com.
2. En la página de inicio de sesión, introduzca el nombre de usuario (**admin**) y la contraseña (**admin**) predeterminados.
3. Ahora puede utilizar la interfaz gráfica del usuario Web (GUI Web) para definir las diferentes configuraciones del router inalámbricos de ASUS.

NOTAS:

- La contraseña predeterminada de inicio de sesión es **admin**. Puede configurar manualmente una nueva contraseña que contenga entre 3 y 16 caracteres alfanuméricos numéricos, tanto en mayúsculas como en minúsculas.
- Si la conexión WAN no está preparada, se le dirigirá a la página Quick Internet Setup (QIS) (Configuración rápida de internet) automáticamente.

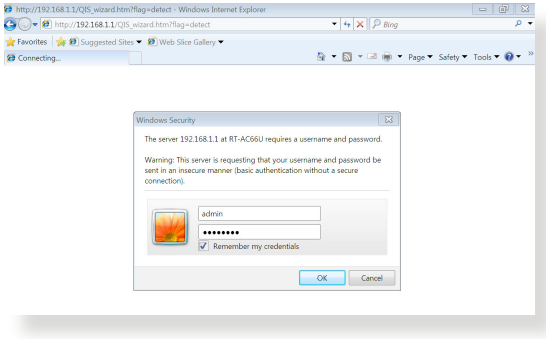
2.2 Función Configuración rápida de Internet (QIS, Quick Internet Setup) con detección automática

La función QIS le ayuda a configurar rápidamente la conexión a Internet.

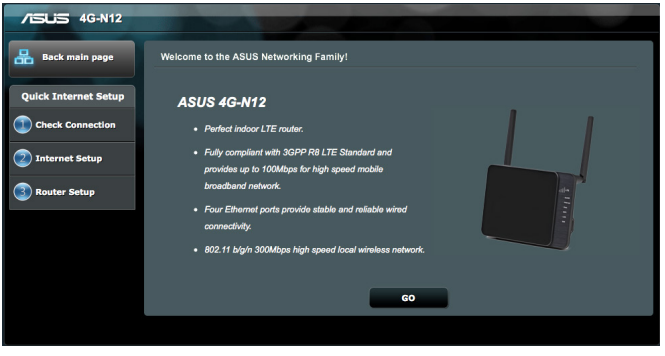
NOTA: Cuando establezca la conexión de Internet por y primera de vez, presione el botón Reiniciar del router inalámbrico para restablecer su configuración predeterminada de fábrica.

Para utilizar QIS con detección automática:

1. Inicie de sesión en la interfaz gráfica del usuario Web. La página QIS se inicia automáticamente.

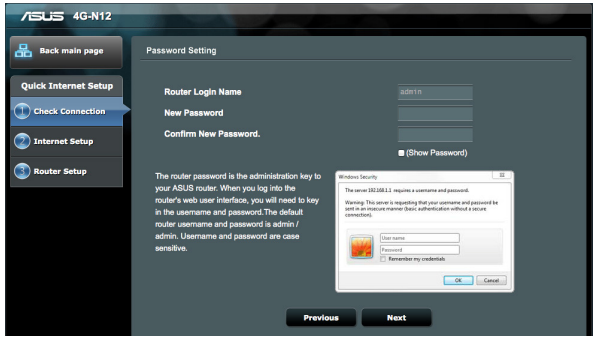

Windows Security
The server 192.168.1.1 at RT-AC66U requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin
Remember my credentials
OK
Cancel

2. La página de bienvenida, haga clic en **Go (Ir)** para continuar.

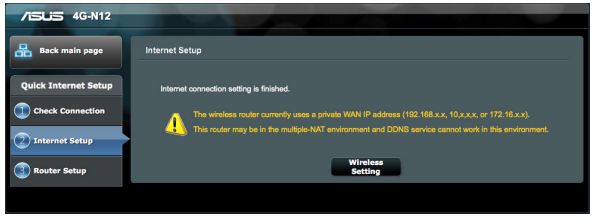

4G-N12
Back main page
Quick Internet Setup
Check Connection
Internet Setup
Router Setup
Welcome to the ASUS Networking Family!
ASUS 4G-N12
Perfect indoor LTE router.
Fully compliant with 3GPP R8 LTE Standard and provides up to 100Mbps for high speed mobile broadband network.
Four Ethernet ports provide stable and reliable wired connectivity.
802.11 b/g/n 300Mbps high speed local wireless network.
GO

3. Cambie la contraseña para el enrutador inalámbrico. Cuando termine, haga clic en **Next (Siguiente)**.

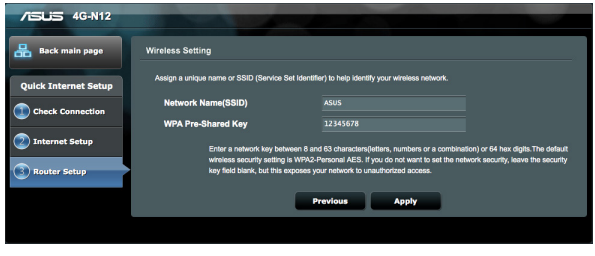
NOTA: Le recomendamos que asigne una contraseña de administrador única para proteger la red contra ataques malintencionados.


4G-N12
Back main page
Password Setting
Quick Internet Setup
Check Connection
Internet Setup
Router Setup
Router Login Name
admin
New Password
Confirm New Password.
(Show Password)
The router password is the administration key to your ASUS router. When you log into the router's web user interface, you will need to key in the username and password.The default router username and password is admin / admin. Username and password are case sensitive.
Previous
Next

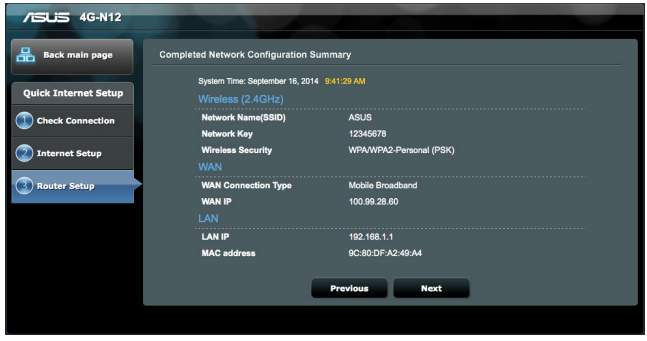
4. El enrutador inalámbrico se detecta y aplica la configuración NPA automáticamente. Cuando termine, haga clic en **WLAN Setting (Configuración WLAN)** para definir la configuración LAN inalámbricas.


4G-N12
Back main page
Internet Setup
Quick Internet Setup
Check Connection
Internet Setup
Router Setup
Internet connection setting is finished.
The wireless router currently uses a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x).
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.
Wireless Setting

5. Asigne un nombre de red único (SSID) y una clave de seguridad de red. Cuando termine, haga clic en **Apply (Aplicar)**.


4G-N12
Back main page
Wireless Setting
Quick Internet Setup
Check Connection
Internet Setup
Router Setup
Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.
Network Name(SSID)
ASUS
WPA Pre-Shared Key
12345678
Enter a network key between 8 and 63 characters(letters, numbers or a combination) or 64 hex digits.The default wireless security setting is WPA2-Personal AES. If you do not want to set the network security, leave the security key field blank, but this exposes your network to unauthorized access.
Previous
Apply

6. Se mostrarán la configuración inalámbrica y de Internet. Haga clic en **Next (Siguiente)** para continuar.



7. Si el asistente no puede aplicar la configuración NPA o se necesita el código PIN de la tarjeta SIM, tendrá que completar la conexión de banda ancha móvil manualmente. Escriba la configuración NPA necesaria y el código PIN de la tarjeta SIM. Cuando termine, haga clic en **Connect (Conectar)**.

NOTA: La detección automática de la conexión de su proveedor de servicio de Internet (ISP) tiene lugar cuando se configura el enrutador inalámbrico por primera vez o cuando se restablece la configuración predeterminada de dicho enrutador.

3 Definir la configuración general

3.1 Utilizar el mapa de red

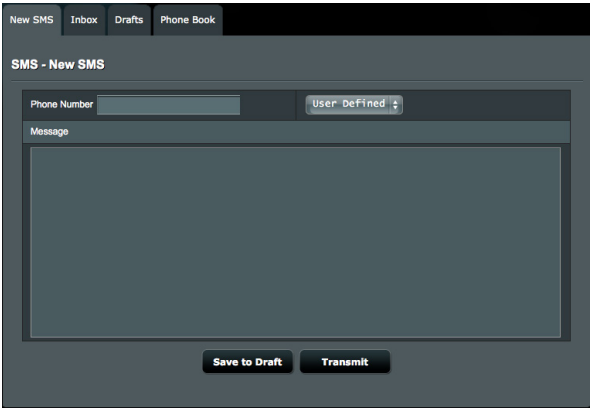
El mapa de red permite comprobar el estado de la conexión de Internet, definir la configuración de seguridad de la red y administrar los clientes de la red.

3.2 SMS

El servicio de mensajes cortos (SMS, Short Message Service) es un servicio de mensajería de texto que permite enviar o recibir mensajes desde el enrutador inalámbrico o en él.

3.2.1 Nuevo SMS

Esta función permite enviar mensajes cortos desde el enrutador inalámbrico.



Para enviar un nuevo mensaje SMS:

1. Escriba el número de teléfono del destinatario.
2. Redacte el mensaje.
3. Haga clic en **Transmit (Transmitir)** para enviar el mensaje.

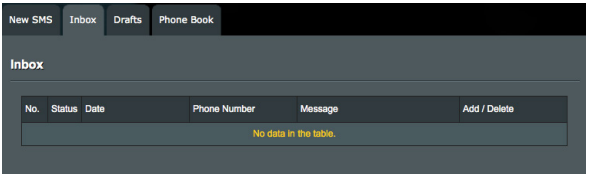
Para guardar un borrador de un mensaje SMS:

1. Escriba el número de teléfono del destinatario.
2. Redacte el mensaje.
3. Haga clic en **Save to Draft (Guardar en borradores)** para guardar el borrador del mensaje.

3.2.2 Bandeja de entrada

La bandeja de entrada le permite ver los mensajes cortos recibidos guardados en el dispositivo.

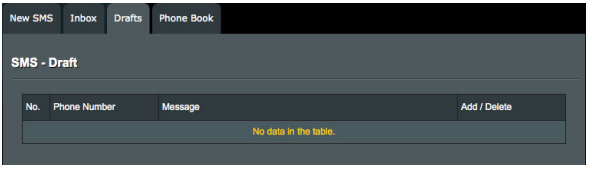
Haga clic en **Read (Leer)** para leer un mensaje o en **Delete (Eliminar)** para eliminar un mensaje.



3.2.3 Borradores

Todos los borradores de mensaje se guardan en el enrutador LTE inalámbrico y se muestran aquí.

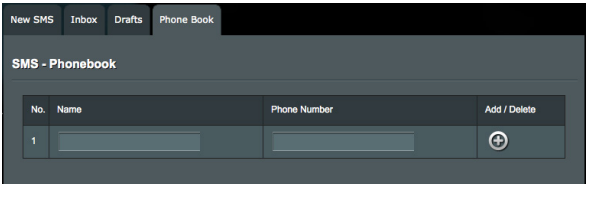
Haga clic en **Transmit (Transmitir)** para leer un mensaje o en **Delete (Eliminar)** para eliminar un mensaje.



3.2.4 Libreta de teléfonos

La libreta de teléfonos de permite guardar los números de teléfono de sus contactos frecuentes.

Para agregar un número de teléfono, escriba el nombre y número de teléfono y haga clic en .



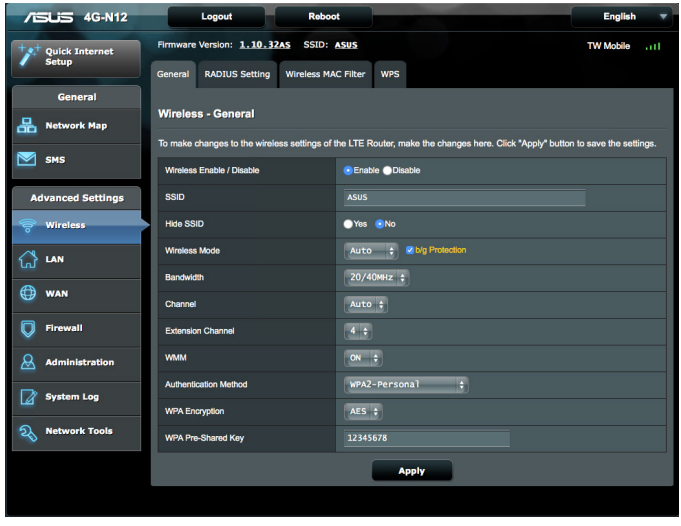
4 Definición de la configuración avanzada

4.1 Inalámbrico

El enrutador LTE inalámbrico funciona como un punto de acceso inalámbrico, permitiendo al dispositivo inalámbrico conectarse a Internet. La interfaz de usuario gráfica permite configurar el canal de radio, el identificador de conjunto de servicios (SSID, Service Set Identifier), la seguridad y la configuración WPS.

4.1.1 General

En la ficha General permite definir la configuración inalámbrica básica.



Para definir la configuración básica inalámbrica:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Wireless (Inalámbrico)** > ficha **General**.
2. **Wireless Enable / Disable (Habilitar o deshabilitar conexión inalámbrica)**: selecciona **Enable (Habilitar)** para utilizar el enrutador como punto de acceso inalámbrico.

3. Asigne un nombre único que contenga 32 caracteres como máximo para su identificador de conjunto de servicios (SSID, Service Set Identifier) o nombre de red para identificar la red inalámbrica. Los dispositivos Wi-Fi pueden identificar la red inalámbrica y conectarse a ella mediante su SSID asignado. Los SSID del título de información se actualizan cuando se guardan nuevos SSID en la configuración.
4. En el campo **Hide SSID (Ocultar SSID)**, seleccione **Yes (Sí)** para impedir que los dispositivos inalámbricos detecten su SSID. Cuando esta función esté habilitada, tendrá que especificar el SSID manualmente en el dispositivo inalámbrico para acceder a la red inalámbrica.
5. Seleccione cualquiera de estas opciones de modo inalámbrico para determinar los tipos de dispositivos inalámbricos que se pueden conectar al router inalámbrico:
   - **Automático**: seleccione **Auto (Automático)** para permitir que los dispositivos 802.11AC, 802.11n, 802.11g y 802.11b se conecten al router inalámbrico.
   - **Heredado**: seleccione **Legacy (Heredado)** para permitir que los dispositivos 802.11b/g/n se conecten al router inalámbrico. Sin embargo, el hardware que admita 802.11n de forma nativa, solamente funcionará a una velocidad máxima de 54 Mbps.
   - **Solo N**: seleccicone **N only (Solo N)** para maximizar el rendimiento N inalámbrico. Este valor impide que los dispositivos 802.11g y 802.11b se conecten al router inalámbrico.
   - **b/g Protection (Protección b/g)**: en la mayoría de las situaciones, el mejor rendimiento se logra con el modo protegido inalámbrico desactivado. Si utiliza el enrutador en un entorno con mucho tráfico 802.11b, 802.11g o muchas interferencias, habilite esta función para garantizar el mejor rendimiento 802.11n.
6. Seleccione cualquiera de estos ancho de banda de canal para acomodar las velocidades de transmisión más altas:

   40 MHz: seleccione este ancho de banda para maximizar el rendimiento inalámbrico.

   20 MHz (predeterminado): seleccione este ancho de banda si tiene problemas con la conexión inalámbrica.

7. Seleccione el canal de funcionamiento para el enrutador inalámbrico. Seleccione **Auto (Automático)** para permitir que el enrutador inalámbrico seleccione automáticamente el canal que tenga la menor cantidad de interferencias.
8. **Extension Channel (Canal de extensión)**: el canal de extensión que puede asignar se basa en lo siguiente:

   Cuando el ancho de banda se establece en 20 MHz, el canal de extensión se deshabilita.

   Cuando el canal inalámbrico (canal principal) se establece en 1, seleccione el canal 5 como el canal de extensión.

   Cuando el canal inalámbrico se establece en el canal 9, seleccione el canal 5 o 13 como el canal de extensión.
9. **WMM**: permite habilitar o deshabilitar el uso de CdS. La función CdS (calidad de servicio) permite diferenciar el tráfico multimedia Wi-Fi (WMM, Wi-Fi Multimedia) y proporcionar un servicio de envío de alta prioridad.
10. Seleccione cualquiera de estos métodos de autenticación:
    - **Sistema abierto**: esta opción no proporciona seguridad.
    - **WPA/WPA2 Personal/WPA Auto-Personal (WPA Autopersonal)**: esta opción proporciona seguridad estricta. Puede utilizar WPA (con TKIP) o WPA2 (con AES). Si selecciona esta opción, debe utilizar cifrado TKIP + AES y especificar la frase de paso WPA (clave de red).
    - **WPA/WPA2 Enterprise (WPA/WPA2 Empresarial)/WPA Auto-Enterprise (WPA Autoempresarial)**: esta opción proporciona seguridad muy estricta. Tiene lugar en un servidor EAP integrado o en un servidor de autenticación RADIUS externo.
11. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.

NOTA: El router inalámbrico admite la tasa máxima de transmisión de 54 Mbps cuando la opción Wireless Mode (Modo inalámbrico) está establecida en Auto (Automático) y la opción Encryption Method (Método de cifrado) es WEP o TKIP.

4.1.2 Configuración de RADIUS

La configuración RADIUS (Remote Authentication Dial In User Service) proporciona un nivel adicional de seguridad cuando se eligen los modos de autenticación WPA-Enterprise (WPA-Empresarial), WPA2-Enterprise (WPA2-Empresarial) o Radius with 802.1x (Radius con 802.1x).

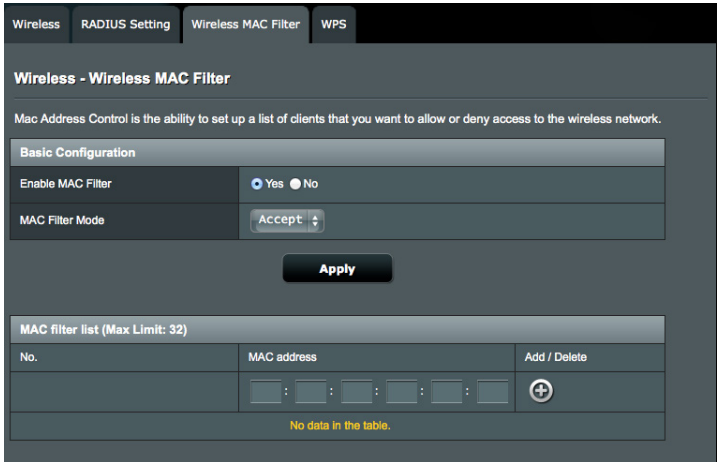
General
RADIUS Setting
Wireless MAC Filter
WPS
Wireless - RADIUS Setting
This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise/ WPA2-Enterprise/ Radius with 802.1x".
Server IP Address
0.0.0.0
Server Port
1812
Connection Secret
Network Key Rotation Interval
2000
(seconds)
Apply

Para definir la configuración de RADIUS inalámbrica:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Wireless (Inalámbrico)** > ficha **RADIUS Setting (Configuración de RADIUS)**.
2. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Wireless (Inalámbrico)** > ficha **RADIUS Setting (Configuración de RADIUS)**.
3. **Server Port (Puerto del servidor:)** escriba el número de puerto del servidor RADIUS en este campo.
4. **Connection Secret (Secreto de conexión)**: escriba la contraseña para acceder al servidor RADIUS.
5. **Network Key Rotation Interval (Intervalo de rotación de claves de red)**: permite definir el período de renovación con el que el servidor RADIUS envía nuevas claves de cifrado a todos los clientes.
6. Cuando termine, haga clic en **Apply (Aplicar)**.

4.1.3 Filtro MAC inalámbrico

El filtro MAC inalámbrico proporciona control sobre los paquetes transmitidos a una dirección MAC (Media Access Control, es decir, Control de acceso al medio) especificada de la red inalámbrica.

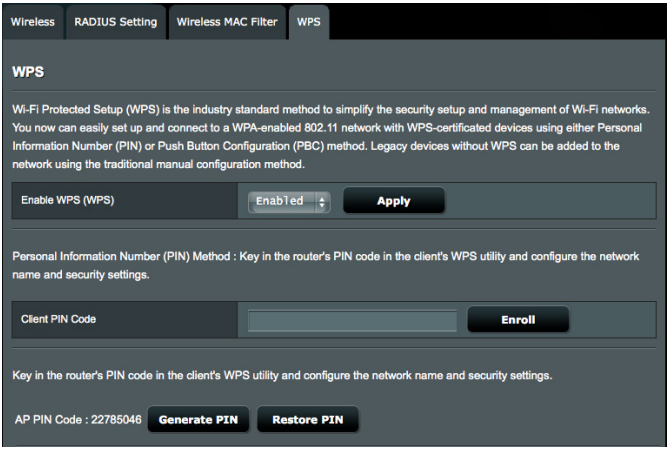


Para configurar el filtro MAC inalámbrico:

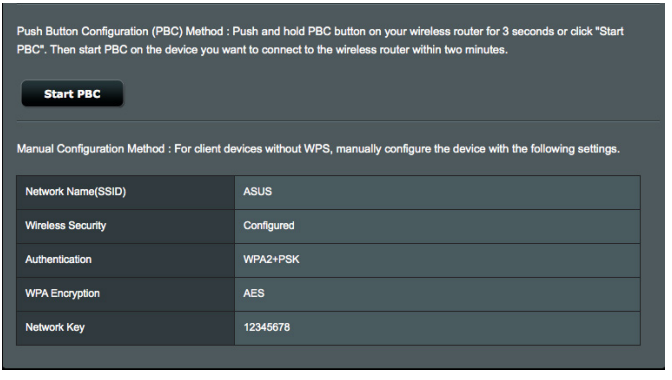
1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Wireless (Inalámbrico)** > ficha **Wireless MAC Filter (Filtro MAC inalámbrico)**.
2. En el campo **Frequency (Frecuencia)**, seleccione la banda de frecuencia que desee utilizar para el filtro MAC inalámbrico.
3. En la lista desplegable **MAC Filter Mode (Modo de filtro MAC)**, seleccione **Accept (Aceptar)** o **Reject (Rechazar)**.
   - Seleccione **Accept (Aceptar)** para permitir que los dispositivos de la lista de filtros MAC accedan a la red inalámbrica.
   - Seleccione **Rejecj (Rechazar)** para impedir que los dispositivos de la lista de filtros MAC accedan a la red inalámbrica.
4. En la lista de filtros MAC, haga clic en el botón **Add (Agregar)** y escriba la dirección MAC del dispositivo inalámbrico.
5. Haga clic en **Apply (Aplicar)**.

4.1.4 WPS (Wi-Fi Protected Setup, es decir, configuración protegida Wi-Fi)

WPS (Wi-Fi Protected Setup, es decir, configuración protegida Wi-Fi) permite crear una red inalámbrica segura fácilmente mediante la función de código PIN o de control de pulsador (PBC, Push Button Control).


Wireless
RADIUS Setting
Wireless MAC Filter
WPS
WPS
Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of Wi-Fi networks. You now can easily set up and connect to a WPA-enabled 802.11 network with WPS-certificated devices using either Personal Information Number (PIN) or Push Button Configuration (PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.
Enable WPS (WPS)
Enabled
Apply
Personal Information Number (PIN) Method : Key in the router's PIN code in the client's WPS utility and configure the network name and security settings.
Client PIN Code
Enroll
Key in the router's PIN code in the client's WPS utility and configure the network name and security settings.
AP PIN Code : 22785046
Generate PIN
Restore PIN

Desplácese hacia abajo para mostrar otros elementos:


Push Button Configuration (PBC) Method : Push and hold PBC button on your wireless router for 3 seconds or click "Start PBC". Then start PBC on the device you want to connect to the wireless router within two minutes.
Start PBC
Manual Configuration Method : For client devices without WPS, manually configure the device with the following settings.
Network Name(SSID)
ASUS
Wireless Security
Configured
Authentication
WPA2+PSK
WPA Encryption
AES
Network Key
12345678

Para habilitar WPS en la red inalámbrica:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Wireless (Inalámbrico)** > ficha **WPS**.
2. En el campo **Enable WPS (Habilitar WPS)**, seleccione **Enabled (Habilitado)** y, a continuación, haga clic en **Apply (Aplicar)**.
3. Configure la funcionalidad WPS a través del método de código PIN o PBC . Consulte los pasos siguientes para obtener más detalles.

Para configurar WPS a través del método de código PIN:

1. Encienda el dispositivo cliente que admite el método de código PIN (Personal Information Number, es decir, números de identificación personal) WPS.
2. Escriba el código PIN del dispositivo cliente y haga clic en **Enroll (Inscribirse)**.

NOTA: El código PIN se puede encontrar en la parte inferior del embalaje o en la interfaz de usuario del dispositivo cliente.

---

3. Inicie el proceso PIN WPS en el dispositivo cliente.

NOTA: Para obtener detalles, consulte el manual de usuario del dispositivo cliente.

---

4. Si desea cambiar el código PIN del router inalámbrico, haga clic en **Generate PIN (Generar PIN)** o **Restore PIN (Restaurar PIN)** para crear o restaurar el PIN.

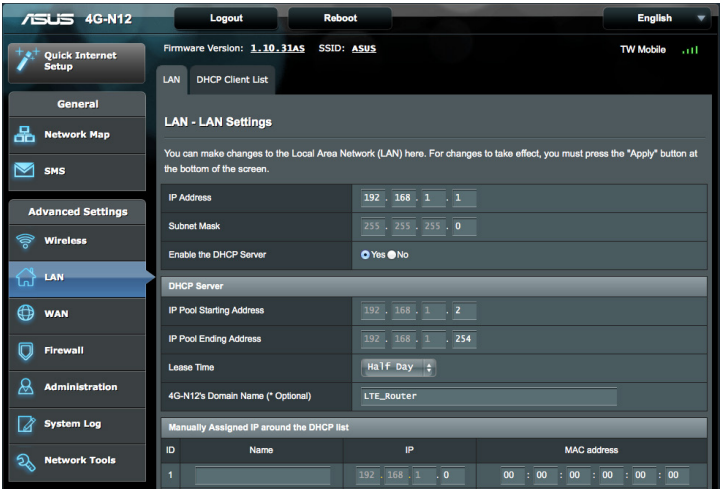
Para configurar WPS a través del método PBC:

1. Encienda el dispositivo cliente compatible con WPS.
2. En la pantalla WPS del router inalámbrico, haga clic en **Start PBC (Iniciar PBC)**. También puede presionar el botón WPS situado en el lado izquierdo del enrutador inalámbrico.
3. Presione el botón WPS del dispositivo cliente.

4.2 LAN

4.2.1 Configuración LAN

La pantalla de configuración LAN le permite definir la dirección IP de la red local del enrutador LTE y modificar la configuración del servidor DHCP.



Para modificar la configuración de dirección IP LAN:

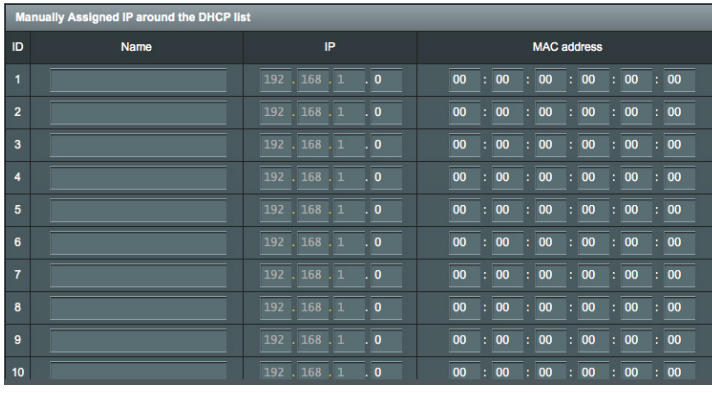
1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **LAN** > ficha **LAN IP (Dirección IP LAN)**.
2. Escriba la dirección IP y la máscara de subred del enrutador inalámbrico.
3. En el campo **Enable the DHCP Server (Habilitar el servidor DHCP)**, seleccione **Yes (Sí)** o **No**. De forma predeterminada, la función DHCP Server (Servidor DHCP) está habilitada.
4. En el campo **IP Pool Starting Address (Dirección inicial del conjunto de direcciones IP)**, escriba la dirección IP inicial.
5. En el campo **IP Pool Ending Address (Dirección final del conjunto de direcciones IP)**, introduzca la dirección IP final.

NOTAS:

- Le recomendamos utilizar el formato de dirección IP 192.168.1.xxx (donde xxx puede ser cualquier número comprendido entre 2 y 254) cuando se especifique un intervalo de direcciones IP.
- Una dirección inicial del conjunto de direcciones IP no debe ser mayor que la dirección final del conjunto de direcciones IP.

6. En la lista desplegable **Lease Time (Tiempo de arrendamiento)**, seleccione la programación para la expiración de una dirección IP. Cuando se alcance esta programación especificada, el servidor DHCP asignará una nueva dirección IP.

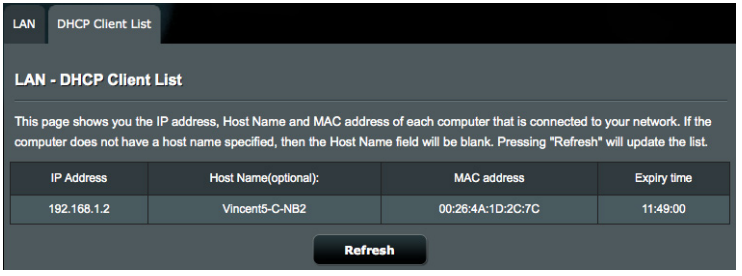
DHCP estático es una función útil que permite asociar un dispositivo de cliente específico con una dirección IP estática de la red. La dirección IP del servidor DHCP se reservará para una dirección MAC única de un dispositivo cliente DHCP basándose en la configuración siguiente.



4.2.2 Lista de clientes DHCP

La pantalla DHCP Client List (Lista de clientes DHCP) muestra la información de los clientes DHCP.

Haga clic en **Refresh (Actualizar)** para actualizar la lista de clientes conectados.


LAN
DHCP Client List
LAN - DHCP Client List
This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing "Refresh" will update the list.
IP Address
Host Name(optional):
MAC address
Expiry time
192.168.1.2
Vincent5-C-NB2
00:26:4A:1D:2C:7C
11:49:00
Refresh

4.3 WAN

El enrutador LTE se implementa con un módulo de evolución a largo plazo (LTE, Long Term Evolution). La red LTE ofrece un ancho de banda de canal amplio comprendido entre 5 MHz y 20 MHz, así como velocidades de datos móviles rápidas de hasta 50 Mbps de subida y 100 Mbps de bajada.

A continuación se muestran las bandas compatibles:

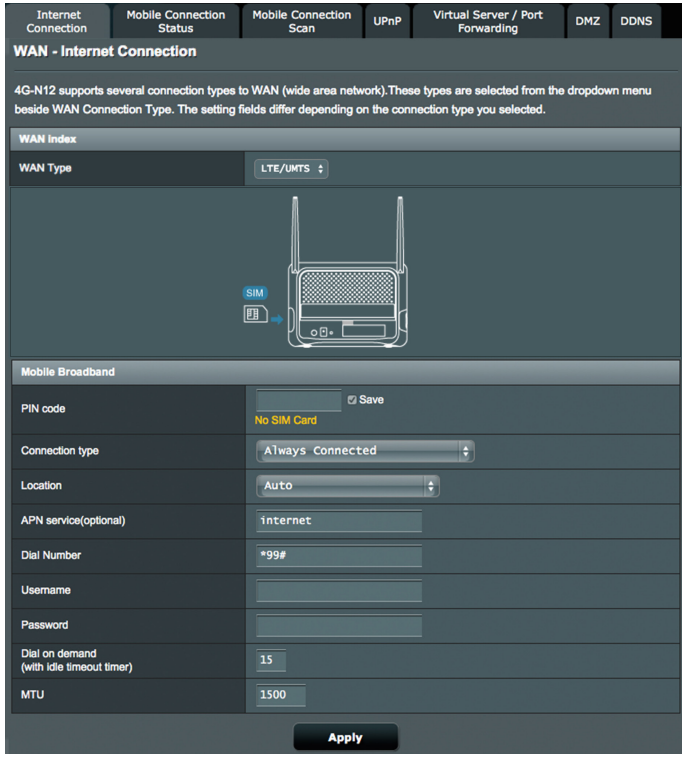
- Banda LTE: FDD B3/7/20
  - LTE Categoría 3: DL: 100 Mbps; UL: 50 Mbps
- UMTS: B1/8
  - HSPA +: DL: 42 Mbps; UL: 5,76 Mbps

4.3.1 Conexión a Internet

Para definir la configuración de la conexión a Internet:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **WAN** > ficha **Internet Connection (Conexión a Internet)**.
2. En el campo **WAN Type (Tipo de WAN)**, seleccione **LTE/UMTS** o **WAN**.

Tipo de WAN - LTE/UMTS



a. Configure las siguientes opciones:

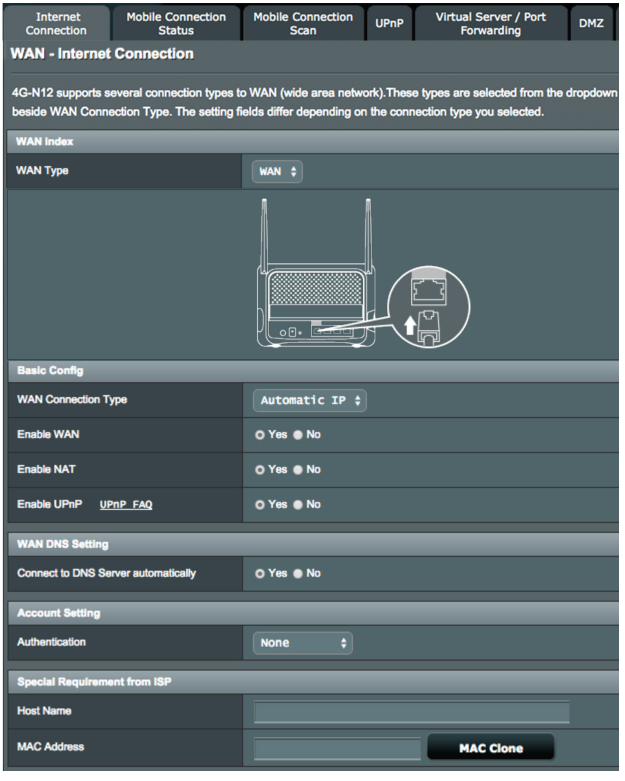
- **PIN Code (Código PIN)**: escriba el código PIN del proveedor 3G/4G.
- **Connection Type (Tipo de conexión)**: este campo permite definir las políticas de conexión. Le recomendamos que seleccione **Auto-Triggered by traffic (Autoactivado por tráfico)** si no utiliza un servicio de datos sin límite.
- **Location (Ubicación)**: seleccione la ubicación del proveedor de servicio 3G/4G en la lista desplegable.
- **APN services (optional) (Servicios NPA (opcional)):**: escriba aquí la información del servicio del nombre del punto de acceso (NPA). Póngase en contacto con su proveedor de servicio 3G/4G para obtener información detallada.
- **Dial Number (Número para marcar)**: escriba el número de acceso del proveedor 3G/4G para la conexión.

- **Username / Password (Nombre de usuario y contraseña)**: escriba el nombre de usuario y la contraseña proporcionados por la compañía de red 3G/4G.
- **Dial on demand (with idle timeout timer) (Marcación bajo demanda (con temporizador de tiempo de espera de inactividad))**: escriba el tiempo (en minutos) transcurrido el cual el enrutador entrará en el modo de suspensión cuando no haya actividad en la red.
- **MTU**: establezca la unidad de transmisión máxima (MTU, Maximum Transmission Unit).

b. Haga clic en **Apply (Aplicar)** para conectarse a la red 3G/4G. El estado de la conexión se mostrará en la pantalla **Mobile Connection Status**.

NOTA: el código PIN puede variar en función del proveedor.

- **Tipo de WAN - WAN**



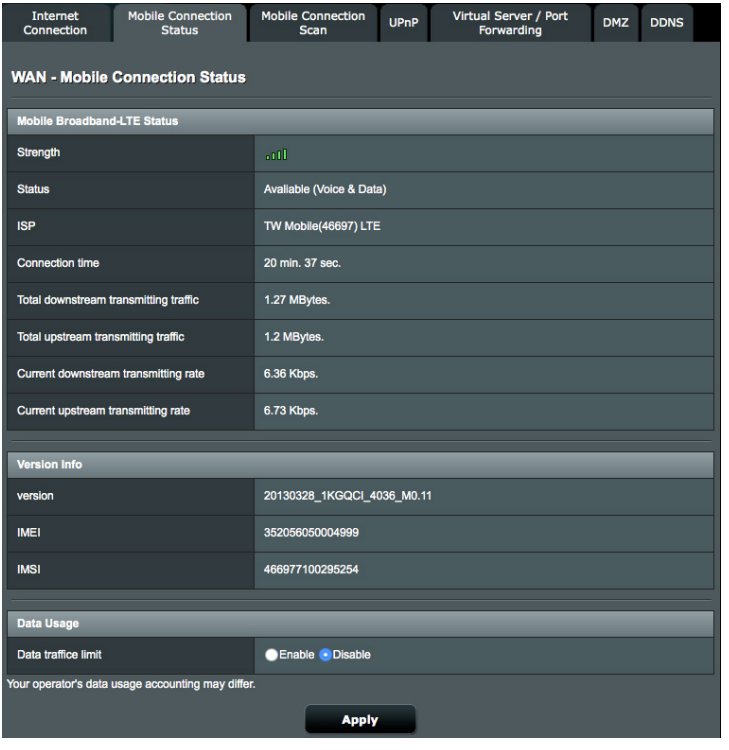
a. Defina la siguiente configuración. Cuando termine, haga clic en **Apply (Aplicar)**.

- **WAN Connection Type (Tipo de conexión WAN)**: Elija el tipo de proveedor de servicio de Internet. Las opciones disponibles son las siguientes: **Automatic IP (Dirección IP automática)**, **PPPoE**, **PPTP**, **L2TP** o **Fixed IP (Dirección IP fija)**. Si el enrutador no es capaz de obtener una dirección IP válida o si usted no está seguro del tipo de conexión WAN, consulte a su ISP.
- **Enable WAN (Habilitar WAN)**: seleccione **Yes (Sí)** para permitir el acceso a Internet del enrutador. Seleccione **No** para deshabilitar el acceso a Internet.
- **Enable NAT (Habilitar NAT)**: NAT (Network Address Translation, es decir, Conversión de direcciones de red) es un sistema en el que una dirección IP pública (IP WAN) se utiliza para proporcionar acceso a Internet a clientes de red con una dirección IP privada en una LAN. La dirección IP privada de cada cliente de red se guarda en una tabla NAT y se utiliza para enrutar paquetes de datos entrantes.
- **Conectar con servidor DNS**: permite a este router obtener la dirección IP DNS de su ISP automáticamente. Un DNS es un sistema central de Internet que convierte los nombres de Internet en direcciones IP numéricas.
- **Autentificación**: este elemento puede ser especificado por algunos ISP. Consulte a su ISP y rellene esta información si es necesario.
- **Nombre de sistema central**: Este campo permite proporcionar un nombre de sistema central para el router. Normalmente es un requisito especial de su ISP. Si su ISP asignó un nombre de equipo central a su PC, especifíquelo aquí.

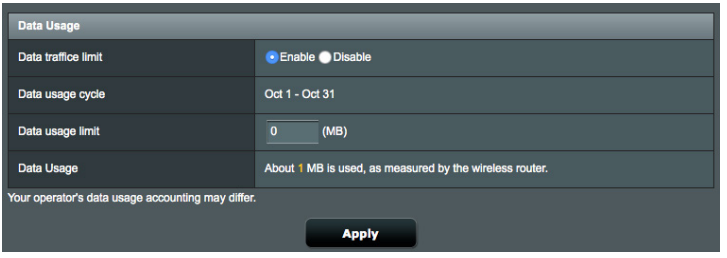
- **Dirección MAC**: la dirección (Media Access Control, es decir, control de acceso al medio) es un identificador único para el dispositivo de red. Algunos ISP supervisan la dirección MAC de los dispositivos de red que se conectan a su servicio y rechazan cualquier dispositivo no reconocido que intente conectarse. Para evitar problemas de conexión debido a una dirección MAC no registrada, puede:
  - Ponerse en contacto con su ISP y actualizar la dirección MAC asociada con su servicios de ISP.
  - Clonar o cambiar la dirección MAC del router inalámbrico de ASUS para que coincida con la dirección MAC del dispositivo de red anterior reconocido por el ISP.

4.3.2 Estado de la conexión móvil

La pantalla Mobile Connection Status (Estado de la conexión móvil) muestra el estado de la conexión detallado de la banda ancha móvil.



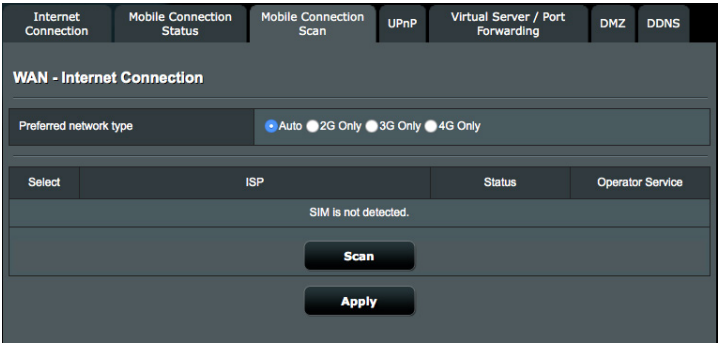
Desplácese hacia abajo para mostrar otros elementos:



Para definir la configuración de uso de datos:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **WAN** > ficha **Mobile Connection Status (Estado de la conexión móvil)**.
2. **Data traffic limit (Límite del tráfico de datos)**: seleccione **Enable (Habilitar)** para poder establecer un límite para el uso de tráfico de Internet.
3. **Data usage limit (Límite del uso de datos)**: establezca un límite superior mensual para el uso de Internet. Cuando el uso de datos alcance el límite, el acceso a Internet se bloqueará.
4. Haga clic en **Apply (Aplicar)**.

4.3.3 Búsqueda de conexión móvil



Para seleccionar la conexión de banda ancha móvil preferida:

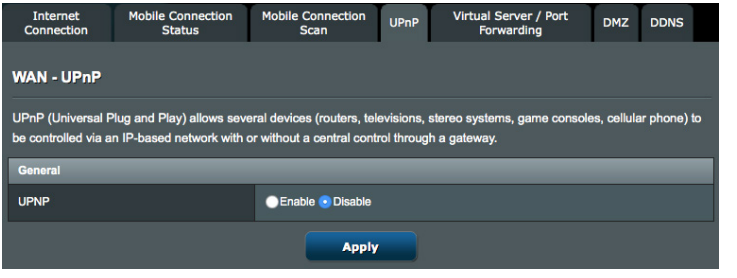
1. En el campo **Preferred network type (Tipo de red preferida)**, seleccione una banda de frecuencia UMTS.
2. Haga clic en **Scan (Buscar)** para mostrar todas las redes móviles disponibles.
3. Seleccione una red móvil y haga clic **Apply (Aplicar)** en para conectarse a ella.

NOTAS:

- El enrutador LTE puede detectar su ISP basándose en la información IMSI de la tarjeta SIM. Si no se encuentra la red móvil de su ISP, conéctese a una red itinerante de otros ISP.
- Si se usa un servicio itinerante se incurrirán en costes adicionales. Pregunte a su proveedor de servicio móvil antes de utilizar el servicio itinerante.

4.3.4 UPnP

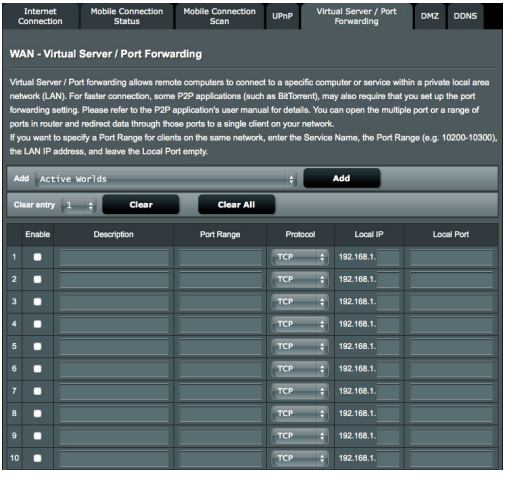
UPnP (Universal Plug and Play, es decir, Conectar y listo universal) permite que varios dispositivos (como por ejemplo enrutadores, televisores, sistemas estéreo, consolas de juego y teléfonos móviles), se controlen a través de una red basada en IP con o sin un centro de control a través de una puerta de enlace. UPnP conecta PC de cualquier tipo de factor de forma, lo cual proporciona una red homogénea para configuración y transferencia de datos remotas. Mediante UPnP, un dispositivo de red se detecta automáticamente. Una vez conectados a la red, los dispositivos se pueden configurar de forma remota para que admitan aplicaciones P2P, juegos interactivos, videoconferencias y servidores Web o proxy. A diferencia del reenvío de puertos, que implica la configuración manual de los puertos, UPnP configura automáticamente el enrutador para aceptar conexiones entrantes y dirigir solicitudes a un PC específico de la red local.


Internet Connection
Mobile Connection Status
Mobile Connection Scan
UPnP
Virtual Server / Port Forwarding
DMZ
DDNS
WAN - UPnP
UPnP (Universal Plug and Play) allows several devices (routers, televisions, stereo systems, game consoles, cellular phone) to be controlled via an IP-based network with or without a central control through a gateway.
General
UPNP
Enable
Disable
Apply

4.3.5 Servidores virtuales/Reenvío de puertos

Servidor virtual es un método para dirigir el tráfico de red desde Internet a un puerto específico o desde un intervalo de puertos específico a un dispositivo o número de dispositivos de una red local.

Si configura el enrutador LTE como servidor virtual, los usuarios remotos que obtengan acceso a tipos de servicio como pueden ser Web o FTP de su sitio local a través de direcciones IP públicas, se podrán redireccionar a servidores locales configurados con direcciones IP privadas. En otras palabras, dependiendo del sitio solicitado (número de puerto TCP/UDP), el enrutador LTE redirecciona la solicitud de servicio externa al servidor adecuado (ubicado en otra dirección IP interna).


Internet Connection
Mobile Connection Status
Mobile Connection Scan
UPnP
Virtual Server / Port Forwarding
DMZ
DDNS
WAN - Virtual Server / Port Forwarding
Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For faster connection, some P2P applications (such as BitTorrent), may also require that you set up the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.
If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200-10300), the LAN IP address, and leave the Local Port empty.
Add
Active Worlds
Add
Clear entry
1
Clear
Clear All
Enable
Description
Port Range
Protocol
Local IP
Local Port
1
2
3
4
5
6
7
8
9
10
TCP
192.168.1.

Por ejemplo, si establece el tipo y el puerto público en TCP y 80, respectivamente (Http o Web) y la dirección IP privada o el puerto en 192.168.2.2:80, todas las solicitudes HTTP procedentes de usuarios externos se transferirán a 192.168.2.2 en el puerto 80. Por tanto, simplemente escribiendo la dirección IP proporcionada por su ISP, los usuarios de Internet podrán acceder al servicio que necesitan en la dirección local a la que se les redirecciona.

NOTA: Los puertos de servicio TCP más comunes son: HTTP: 80, FTP: 21, Telnet: 23 y POP3: 110. En http://www.iana.org/assignments/port-numbers encontrará una lista de puertos.

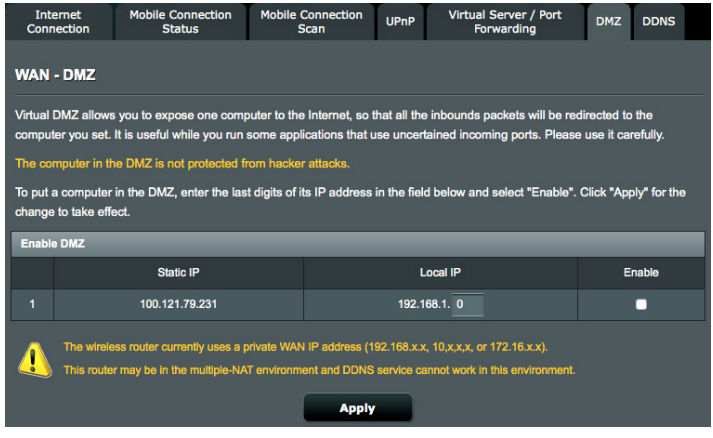
4.3.6 DMZ

DMZ virtual expone un cliente a Internet, permitiendo a dicho cliente recibir todos los paquetes entrantes dirigidos a la red de área local.

El tráfico entrante procedente de Internet se suele descartar y enrutar a un cliente específico solamente si el reenvío de puertos o un activador de puertos se ha configurado en la red. En una configuración DMZ, un cliente de recibe todos los paquetes entrantes.

La configuración de DMZ en una red resulta de gran utilidad cuando necesita abrir puertos entrantes o desea hospedar un servidor de dominio, Web o de correo electrónico.

Precaución: la apertura de todos los puertos de un cliente a Internet hace que la red sea vulnerable a ataques externos. Sea consciente de los riesgos de seguridad que implica utilizar DMZ.


Internet Connection
Mobile Connection Status
Mobile Connection Scan
UPnP
Virtual Server / Port Forwarding
DMZ
DDNS
WAN - DMZ
Virtual DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set. It is useful while you run some applications that use uncertained incoming ports. Please use it carefully.
The computer in the DMZ is not protected from hacker attacks.
To put a computer in the DMZ, enter the last digits of its IP address in the field below and select "Enable". Click "Apply" for the change to take effect.
Enable DMZ
Static IP
Local IP
Enable
1
100.121.79.231
192.168.1. 0
The wireless router currently uses a private WAN IP address (192.168.x.x, 10,x,x,x, or 172.16.x.x).
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.
Apply

Para configurar DMZ:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **WAN** > ficha **DMZ**.
2. Defina la siguiente configuración. Cuando haya finalizado, haga clic en **Apply (Aplicar)**.

- **Enable DMZ (Habilitar DMZ):** escriba el último dígito la dirección IP LAN del cliente que proporcionará el servicio DMZ y que se expondrá en Internet. Asegúrese de que el servidor tiene una dirección IP estática. Active la casilla **Enable (Habilitar)**.

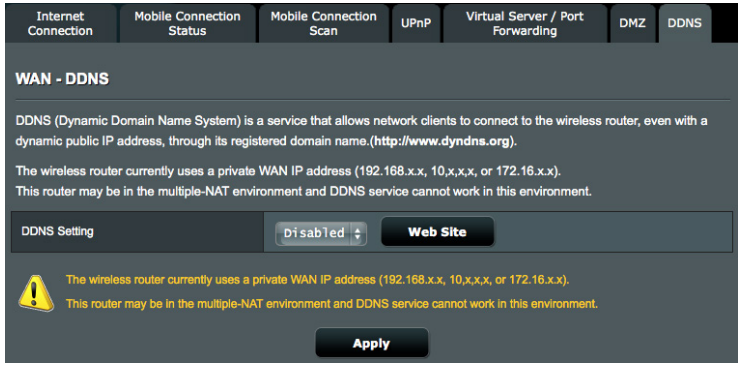
Para quitar DMZ:

1. Desactive la casilla **Enable (Habilitar)** y haga clic en **Apply (Aplicar)**.

4.3.7 DDNS

La configuración del sistema de nombres de dominio dinámico (DDNS, Dynamic Domain Name System) permite acceder al enrutador fuera de la red a través del servicio DDNS proporcionado. El servicio DDNS, que asigna un nombre de dominio a una dirección IP estática o dinámica, está desarrollado por DynDNS.org.

Con una conexión DDNS, puede hospedar un sitio Web, un servidor de correo electrónico, un sitio FTP y otras aplicaciones de Internet en la red de área local incluso cuando utiliza direcciones IP dinámicas para los nombres de dominio.


Internet Connection
Mobile Connection Status
Mobile Connection Scan
UPnP
Virtual Server / Port Forwarding
DMZ
DDNS
WAN - DDNS
DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name.(http://www.dyndns.org).
The wireless router currently uses a private WAN IP address (192.168.x.x, 10,x,x,x, or 172.16.x.x).
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.
DDNS Setting
Disabled
Web Site
The wireless router currently uses a private WAN IP address (192.168.x.x, 10,x,x,x, or 172.16.x.x).
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.
Apply

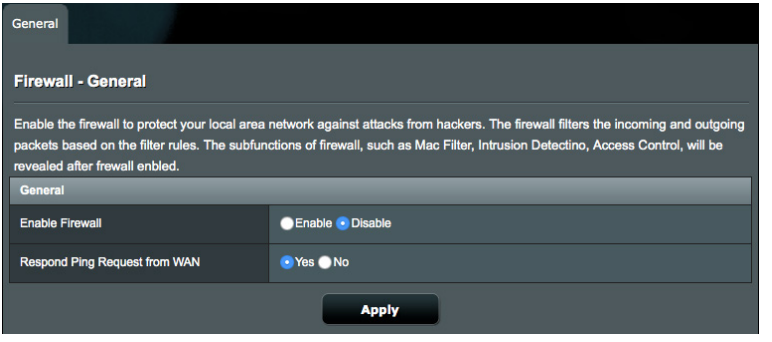
Para configurar DDNS:

1. Seleccione **DDNS Setting (Configuración DDNS)** en la lista desplegable y haga clic en **Web Site (Sitio Web)** para ir al sitio Web DynDNS.org.
2. Complete el registro en el sitio Web DDNS.
3. Escriba el nombre de usuario la contraseña y el nombre de dominio de la configuración DDNS.
4. Haga clic en **Update Dynamic DNS (Actualizar DNS dinámico)** para actualizar la configuración de la dirección IP.
5. Cuando termine, haga clic en **Apply (Aplicar)**.

4.4 Firewall

4.4.1 General

El enrutador inalámbrico puede actuar como un firewall de hardware para la red. Configure el firewall para proteger la red contra ataques malintencionados, como por ejemplo, ataques de tipo Denegación de servicio (DdS). Los ataques DdS deshabilitan un dispositivo o red para denegar el acceso de los usuarios a los recursos de la red.

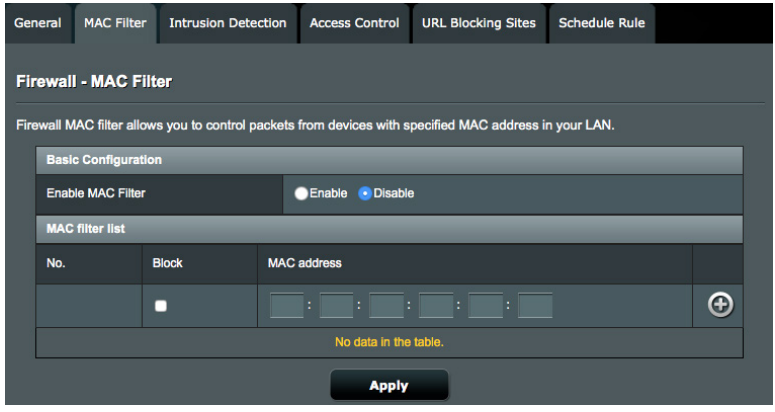

General
Firewall - General
Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules. The subfunctions of firewall, such as Mac Filter, Intrusion Detectino, Access Control, will be revealed after frewall enbled.
General
Enable Firewall
Enable
Disable
Respond Ping Request from WAN
Yes
No
Apply

Para definir configuración básica de Firewall:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Firewall** > ficha **General**.
2. En el campo **Enable Firewall (Habilitar Firewall)**, seleccione **Enable (Habilitar)**.
3. En el campo **Respond Ping Request from WAN (Responder a la solicitud Ping desde WAN)**, seleccione **Yes (Sí)** para impedir que los usuarios malintencionados ejecuten el comando Ping en dispositivos de la red desde Internet.
4. Haga clic en **Apply (Aplicar)**.

4.4.2 Filtro MAC

Cuando la opción MAC Filter (Filtro MAC) está habilitada, solamente las direcciones MAC que se encuentren en la lista se les concederá o rechazará el acceso a la red.

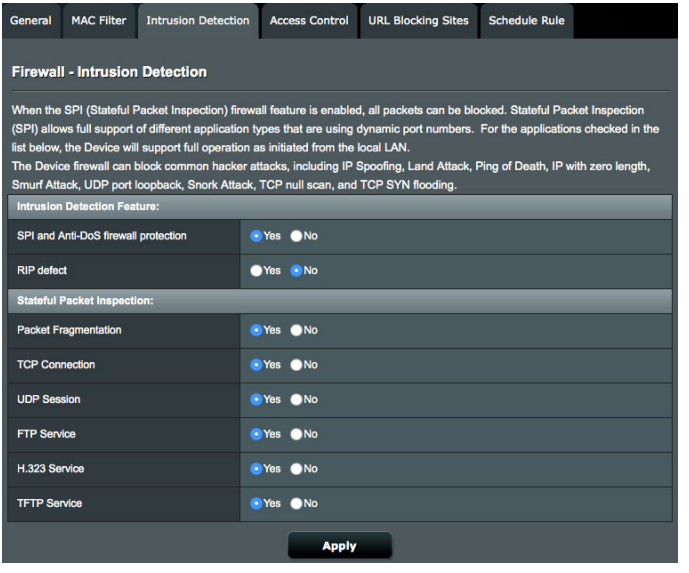


Para configurar un filtro de direcciones MAC:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Firewall** > ficha **MAC Filter (Filtro MAC)**.
2. En el campo **Enable MAC Filter (Habilitar filtro MAC)**, seleccione **Enable (Habilitar)**.
3. Escriba una dirección MAC y haga clic en el botón .
4. Haga clic en **Apply (Aplicar)**.

4.4.3 Detección de intrusiones

La función de detección de intrusiones bloquea e impide que ataques malintencionados o intrusiones dañen la red y los dispositivos conectados a ella. El enrutador inalámbrico impide ataques DdS, como por ejemplo, falsificación de dirección IP, Ping de muerte, IP con longitud cero, ataque Smurf, bucle de puerto UDP, ataque Snork, búsqueda nula TCP e inundación de sincronismo TCP.


General
MAC Filter
Intrusion Detection
Access Control
URL Blocking Sites
Schedule Rule
Firewall - Intrusion Detection
When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Device will support full operation as initiated from the local LAN.
The Device firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.
Intrusion Detection Feature:
SPI and Anti-DoS firewall protection
Yes No
RIP defect
Yes No
Stateful Packet Inspection:
Packet Fragmentation
Yes No
TCP Connection
Yes No
UDP Session
Yes No
FTP Service
Yes No
H.323 Service
Yes No
TFTP Service
Yes No
Apply

Función de detección de intrusiones

SPI and Anti-DoS firewall protection (SPI y protección de firewall anti-DdS): cuando este elemento está habilitado, todos los paquetes entrantes procedentes de los servicios WAN se bloquean excepto aquellos tipos seleccionados en la sección Stateful Packet Inspection (SPI) (Inspección de paquetes con información de estado).

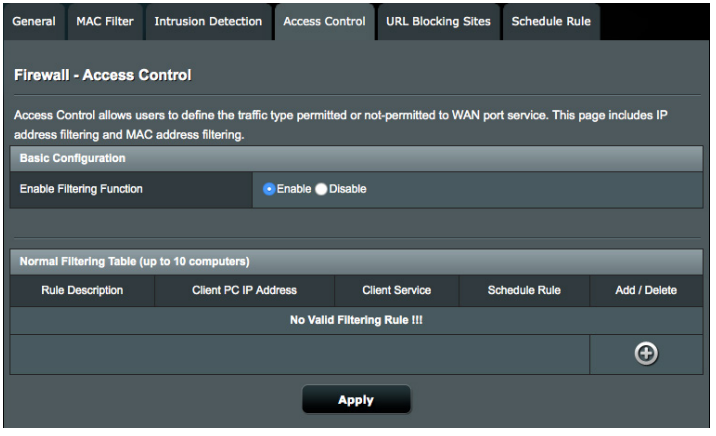
RIP defect (Defecto RIP): cuando este elemento está habilitado, el enrutador no bloquea los paquetes de solicitud RIP procedentes de los servicios WAN, evitando así el desbordamiento de las colas de entrada debido a la acumulación de paquetes.

Nspección de paquetes con información de estado

Seleccione **Yes (Sí)** para permitir que un determinado tipo de tráfico atraviese el firewall o **No** para bloquear el tipo de tráfico.

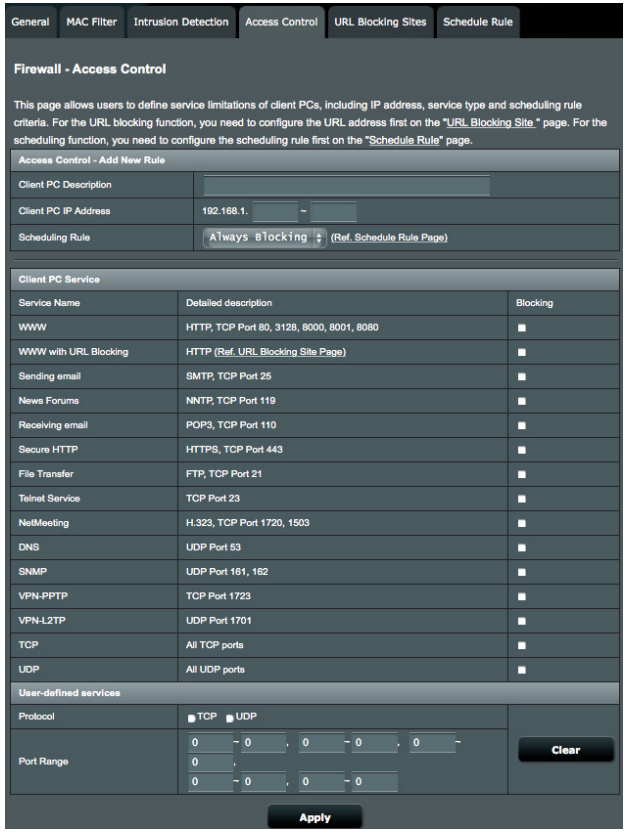
4.4.4 Control de acceso

El control de acceso permite especificar los clientes o servicios a los que se les permite o impide usar el servicio de puertos WAN. Las reglas de control de acceso se ejecutan con las programaciones especificadas.



Para configurar un filtro de servicio de red:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Firewall** > ficha **Access Control (Control de acceso)**.
2. En el campo **Enable MAC Filter (Habilitar filtro MAC)**, seleccione **Enable (Habilitar)**.
3. Haga clic en el botón para iniciar la pantalla Add New Rule (Agregar nueva regla).

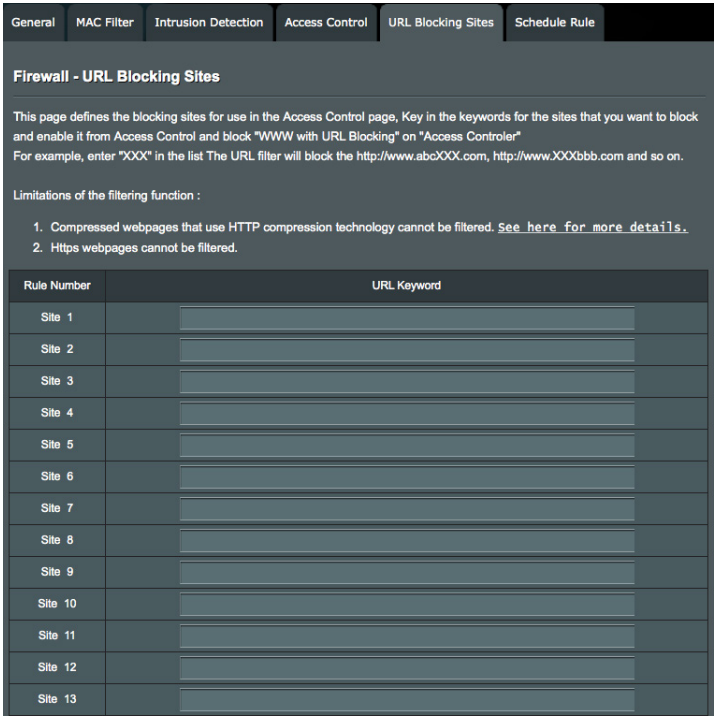


4. Escriba una descripción para los clientes.
5. Escriba el intervalo de direcciones IP del cliente para bloquear los clientes especificados.
6. Defina una regla de programación. Puede seleccionar Always Blocking (Bloquear siempre) o especificar el día y la hora en los que los filtros se activarán.
7. Para especificar un servicio de red para filtrar, selecciónelo y active **Blocking (Bloquear)** en **Client PC Service (Servicio de PC de cliente)** para bloquear el servicio de red predefinido.
8. En el campo **User-defined services (Servicios definidos por el usuario)**, seleccione un tipo de protocolo y escriba los intervalos de direcciones IP de los clientes para definir manualmente los clientes que se bloquearán.
9. Haga clic en **Apply (Aplicar)**.

4.4.5 Filtro de direcciones URL

Puede especificar palabras claves o direcciones Web para indicar direcciones URL.

NOTA: El filtro de direcciones URL se basa en una consulta DNS. Si el cliente de red ya ha accedido a un sitio Web, como por ejemplo, http://www.abcxxx.com, dicho sitio no se bloqueará (una memoria DNS del sistema almacena los sitios Web previamente visitados). Para resolver este problema, borre la memoria DNS antes de configurar el filtro de direcciones URL.


General
MAC Filter
Intrusion Detection
Access Control
URL Blocking Sites
Schedule Rule
Firewall - URL Blocking Sites
This page defines the blocking sites for use in the Access Control page, Key in the keywords for the sites that you want to block and enable it from Access Control and block "WWW with URL Blocking" on "Access Controler"
For example, enter "XXX" in the list The URL filter will block the http://www.abcXXX.com, http://www.XXXbbb.com and so on.
Limitations of the filtering function :
1. Compressed webpages that use HTTP compression technology cannot be filtered. See here for more details.
2. Https webpages cannot be filtered.
Rule Number
URL Keyword
Site 1
Site 2
Site 3
Site 4
Site 5
Site 6
Site 7
Site 8
Site 9
Site 10
Site 11
Site 12
Site 13

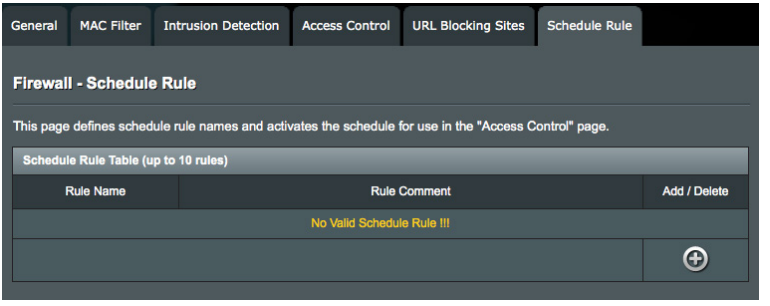
Para configurar un filtro de direcciones URL:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Firewall** > ficha **URL Filter (Filtro de direcciones URL)**.
2. Escriba una palabra clave URL.
3. Haga clic en **Apply (Aplicar)**.

4.4.6 Regla de programación

Cada regla de control de acceso se puede activar a una hora programada previamente definida.

Puede definir la regla de programación en la página **Schedule Rule (Regla de programación)** y aplicarla en la página **Access Control (Control de acceso)**.


General
MAC Filter
Intrusion Detection
Access Control
URL Blocking Sites
Schedule Rule
Firewall - Schedule Rule
This page defines schedule rule names and activates the schedule for use in the "Access Control" page.
Schedule Rule Table (up to 10 rules)
Rule Name
Rule Comment
Add / Delete
No Valid Schedule Rule !!!

4.5 Administración

4.5.1 Sistema

La página **System (Sistema)** permite definir la configuración inalámbrica del router

Para definir la configuración del sistema:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Administration (Administración)** > ficha **System (Sistema)**.
2. Puede configurar los ajustes parámetros:
   - **Administrator Password (Contraseña de administrador)**: puede cambiar la contraseña y el nombre de inicio de sesión para el router inalámbrico introduciendo un nombre y contraseña nuevos.
     - **Login Timeout (Tiempo de espera de inicio de sesión)**: la mayoría de los administradores Web establecen esta propiedad en 10 minutos. No se debe establecer en un valor superior a 20 minutos (excepto en casos excepcionales) porque cada sesión abierta se hospeda en memoria.
   - **Time and Time Zone (Hora y zona horaria)**: Seleccione la hora y la zona horaria para la red.
     - **Zona horaria**: ajuste la zona horaria conforme a la ubicación del enrutador.
     - **Daylight Saving Time (DST) (Horario de verano)**: si la región adopta el horario de verano (DST), habilite esta opción.
     - **Servidor NTP**: el router inalámbrico puede acceder a un servidor NTP (Network time Protocol, es decir, Protocolo de hora de red) para sincronizar la hora.
   - **Web Access from WAN (Acceso Web desde WAN):**
     - **Enable Web Access from (Habilitar acceso Web desde)**: seleccione **Enable (Habilitar)** para permitir que los dispositivos que se encuentran fuera de la red accedan a la configuración GUI del enrutador inalámbrico. Seleccione **Disable (Deshabilitar)** para impedir el acceso.
     - **Permitted IP Address (Dirección IP permitida)**:
       - **Any IP address can remotely manage the wireless router (Cualquier dirección IP puede administrar el enrutador inalámbrico en remoto).**
       - **Only allow specific IP (Permitir solo direcciones IP específicas)**: especifique las direcciones IP WAN de dispositivos de red a los que se permite acceder a la configuración del enrutador inalámbrico desde WAN.

- **Port of Web Access from WAN (Puerto de acceso Web desde WAN)**: especifique el número de puerto del servidor Web al que se le permite acceder a la configuración del enrutador inalámbrico.

3. Haga clic en **Apply (Aplicar)**.

4.5.2 Actualización del firmware

NOTA: Descargue la versión más reciente del firmware del sitio Web de ASUS, a través de la dirección **http://www.asus.com**

Para actualizar el firmware:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Administration (Administración)** > ficha **Firmware Upgrade (Actualizar firmware)**.
2. En el campo **New Firmware File (Nuevo archivo de firmware)**, haga clic en **Browse (Examinar)** para buscar el archivo descargado.
3. Haga clic en **Upload (Enviar)**.

NOTA: Cuando el proceso de actualización se complete, espere un poco para que el sistema se reinicie.

4.5.3 Restaurar / Guardar / Enviar configuración

Para restaurar / guardar / enviar la configuración:

1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > **Administration (Administración)** > ficha **Restore/Save/Upload Setting (Restaurar, guardar o cargar configuración)**.
2. Seleccione las tareas que desee realizar:
   - Para restaurar la configuración predeterminada de fábrica haga clic en **Restore (Restaurar)** y después en **OK (Aceptar)** en el mensaje de confirmación.
   - Para guardar la configuración del sistema actual, haga clic en **Save (Guardar)**, desplácese a la carpeta en la que pretende guardar el archivo y, por último, haga clic en **Save (Guardar)**.
   - Para restaurar la configuración anterior del sistema, haga clic en **Browse (Explorar)** para localizar el archivo que desee restaurar y haga clic en **Upload (Enviar)**.

Si se producen problemas, cargue la versión de firmware más reciente y defina la nueva configuración. No restaure la configuración predeterminada del router.

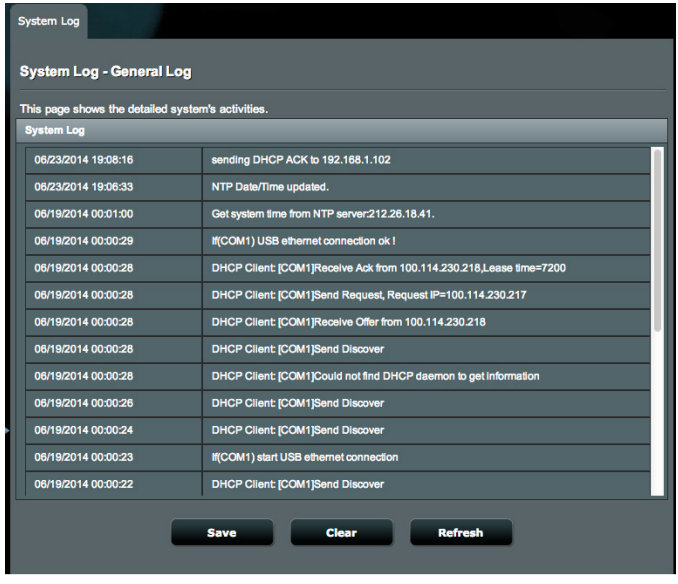
4.6 Registro del sistema

El registro del sistema contiene las actividades de red grabadas.

NOTA: el registro el sistema se restablece cuando el router se reinicia o apaga.

Para ver el registro del sistema:

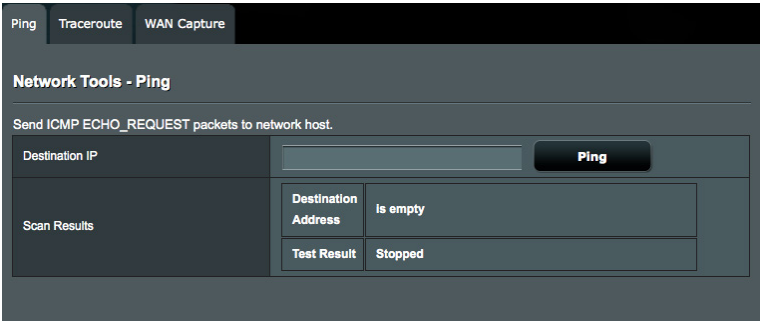
1. En el panel de navegación, vaya a **Advanced Settings (Configuración avanzada)** > ficha **System Log (Registro del sistema)**.
2. En esta página puede ver las actividades de la red:
3. (Opcional) Haga clic en **Save (Guardar)** para exportar los registros del sistema.


System Log
System Log - General Log
This page shows the detailed system's activities.
System Log
06/23/2014 19:08:16 sending DHCP ACK to 192.168.1.102
06/23/2014 19:06:33 NTP Date/Time updated.
06/19/2014 00:01:00 Get system time from NTP server:212.26.18.41.
06/19/2014 00:00:29 If(COM1) USB ethernet connection ok !
06/19/2014 00:00:28 DHCP Client: [COM1]Receive Ack from 100.114.230.218,Lease time=7200
06/19/2014 00:00:28 DHCP Client: [COM1]Send Request, Request IP=100.114.230.217
06/19/2014 00:00:28 DHCP Client: [COM1]Receive Offer from 100.114.230.218
06/19/2014 00:00:28 DHCP Client: [COM1]Send Discover
06/19/2014 00:00:28 DHCP Client: [COM1]Could not find DHCP daemon to get information
06/19/2014 00:00:26 DHCP Client: [COM1]Send Discover
06/19/2014 00:00:24 DHCP Client: [COM1]Send Discover
06/19/2014 00:00:23 If(COM1) start USB ethernet connection
06/19/2014 00:00:22 DHCP Client: [COM1]Send Discover
Save
Clear
Refresh

4.7 Herramientas de red

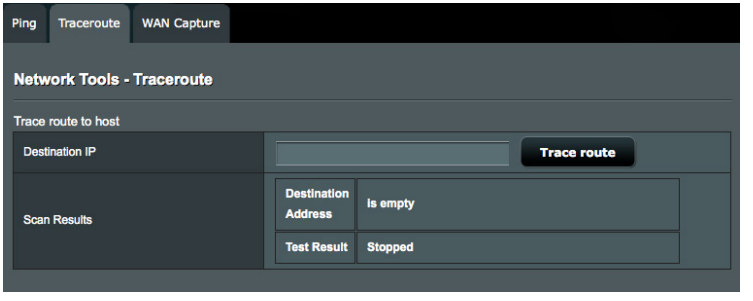
4.7.1 Ping

Una prueba ping determina la latencia (retardo de comunicación) entre el enrutador ASUS y otro servidor (como por ejemplo www.google.com) en una red enviando varios paquetes ICMP y escuchando las respuestas. Escriba un nombre de host o dirección IP para realizar un Ping. Los resultados de la prueba muestran el tiempo de ida y vuelta más corto, medio y máximo y la tasa de pérdida de paquetes entre hosts.



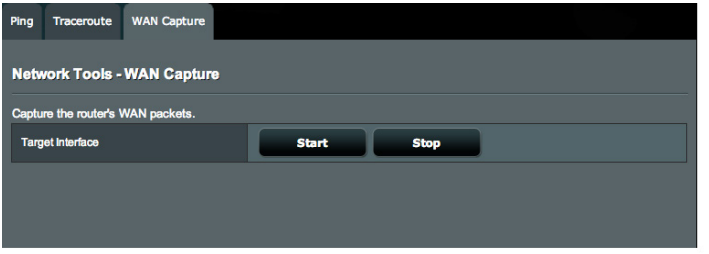
4.7.2 Traceroute

La prueba Traceroute (también conocida como ruta de seguimiento o tracert) trazará la ruta que toman los paquetes de prueba de un destino de servidor a otro. Los resultados de la prueba proporcionan una lista de hosts o direcciones IP que muestran la ruta que toman los paquetes de prueba empezando desde la ubicación de supervisión seleccionada hasta el dominio o dirección IP de destino (como por ejemplo www.google.com). Normalmente, la prueba Traceroute se utiliza para solucionar problemas de red y para identificar los problemas de enrutamiento o los firewalls que pueden estar bloqueando el acceso a un sitio web.



4.7.3 Captura WAN

La función WAN Capture (Captura WAN) permite capturar todos los paquetes que atraviesan la red de banda ancha móvil.



Para capturar los paquetes WAN del enrutador:

1. Para comenzar a capturar los paquetes, haga clic en **Start (Inicio)**. El explorador comenzará a descargar el archivo pktDump.cap al equipo.
2. Para detener la captura de los paquetes, haga clic en **Stop (Detener)**. El explorador terminará de capturar los paquetes y completará la descarga del archivo pktDump.cap.

NOTA: Se necesita una aplicación externa como Wireshark para ver los paquetes capturados en el archivo.

5 Preguntas más frecuentes (P+F)

No puedo acceder a la GUI del router mediante un explorador Web.

- **Configuración del hardware:**
  - Si el equipo está conectado mediante cables, compruebe la conexión del cable Ethernet y el estado de los LED.

- **Error al iniciar sesión:**
  - Asegúrese de que utiliza la información de inicio de sesión correcta. El nombre y la contraseña de inicio de sesión predeterminados de fábrica son "admin/admin". Asegúrese de que la tecla Bloq Mayús está deshabilitada al introducir la información de inicio de sesión.

- **La memoria caché DNS da un resultado de DNS incorrecto:**
  - Elimine las cookies y los archivos del explorador Web.

- **Configuración de conexión anterior:**
  - Deshabilite el servidor proxy si se encuentra habilitado.
  - Establezca la configuración TCP/IP del equipo para que reciba una dirección IP automáticamente.
  - Deshabilite todas las conexiones de acceso telefónico, si hay alguna habilitada.

NOTAS:

- Los comandos para eliminar cookies y archivos varían en función de los exploradores Web.
- Deshabilite la configuración del servidor proxy, cancele la conexión de acceso telefónico a redes y establezca la configuración TCP/IP para obtener la dirección IP automáticamente. Para obtener más detalles, consulte el capítulo 1 de este manual del usuario.

El cliente no puede establecer una conexión inalámbrica con el router.

- **Se encuentra fuera del alcance de la red:**
  - Coloque el router más cerca del cliente inalámbrico.
  - Intente ajustar las antenas del router hacia la mejor dirección tal y como se describe en la sección **1.4 Ubicar el router**.
- **El servidor DHCP se ha deshabilitado:**
  1. Inicie la GUI Web. Vaya a **General** > **Network Map (Mapa de red)**> **Clients (Clientes)** y busque el dispositivo que desee conectar al router.
  2. Si no puede encontrar el dispositivo en **Network Map (Mapa de red)**, vaya a **Advanced Settings (Configuración avanzada)**> **LAN** > **DHCP Server (Servidor DHCP)**, lista **Basic Config (Configuración básica)**, seleccione **Yes (Sí)** en **Enable the DHCP Server (Habilitar el servidor DHCP)**.
- **No se puede encontrar el SSID:**
  - Si está utilizando un adaptador LAN inalámbrico, compruebe si el canal inalámbrico en uso es conforme a los canales disponibles en su país o área. Si no lo es, ajuste el canal, el ancho de banda y el modo inalámbrico.
- Si sigue sin poder conectarse al router de forma inalámbrica, puede restablecer la configuración predeterminada de fábrica de dicho router. En la GUI del router, haga clic en **Administration (Administración)** > **Restore/Save/Upload Setting (Restaurar, guardar y cargar configuración)** y haga clic en **Restore (Restaurar)**.

No es posible acceder a Internet.

- Compruebe si el router se puede conectar a la dirección IP WAN de su ISP. Para ello, inicie la GUI Web y vaya a **General**> **Network Map (Mapa de red)** y compruebe **Internet Status (Estado de Internet)**.
- Si todavía no tiene acceso a Internet, intente reiniciar el equipo y compruebe la dirección IP y la dirección de la puerta de enlace de la red.

- Compruebe los indicadores de estado del modem ADSL y del router inalámbrico. Si el LED WAN del router inalámbrico no está ENCENDIDO, compruebe si todos los cables están enchufados correctamente.

Olvidó el SSID (nombre de red) o la contraseña de red

- Configure un nuevo SSID y una nueva clave de cifrado mediante la conexión cableada (cable Ethernet). Inicie la GUI Web, vaya a **Network Map (Mapa de red)**, haga clic en el icono de router, especifique un nuevo SSID y una nueva clave de cifrado y, a continuación, haga clic en **Apply (Aplicar)**.
- Restablezca la configuración predeterminada del router. Inicie la GUI Web, haga clic en **Administration (Administración)** > **Restore/Save/Upload Setting (Restaurar, guardar y cargar configuración)** y haga clic en **Restore (Restaurar)**. Tanto la cuenta como la contraseña de inicio de sesión predeterminadas son "admin".

¿Cómo restaurar el sistema a su configuración predeterminada?

- Vaya a **Administration (Administración)** > **Restore/Save/Upload Setting (Restaurar, guardar y cargar configuración)** y haga clic en **Restore (Restaurar)**.

  A continuación se indican los valores predeterminados de fábrica del dispositivo:

Nombre de usuario:	admin
Contraseña:	admin
Habilitar DHCP:	Sí
Dirección IP:	192.168.1.1
Nombre de dominio:	(Vacío)
Máscara de subred:	255.255.255.0
Servidor DNS 1:	192.168.1.1
Servidor DNS 2:	(Vacío)
Identificador SSID (2.4GHz):	ASUS

Apéndices

Notas

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to http://csr.asus.com/english/Takeback.htm for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

http://csr.asus.com/english/index.aspx

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements – Article 3

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 & EN 301 893 have been conducted. These are considered relevant and sufficient.

CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Canada, Industry Canada (IC) Notices

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

The radiated output power of the ASUS Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has been evaluated for and shown compliant with the IC Specific Absorption Rate ("SAR") limits when installed in specific host products operated in portable exposure conditions (antennas are less than 20 centimeters of a person's body).

This device has been certified for use in Canada. Status of the listing in the Industry Canada's REL (Radio Equipment List) can be found at the following web address: http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng

Additional Canadian information on RF exposure also can be found at the following web: http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003 et RSS-210.

Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent a ecter son fonctionnement.

NCC 警語

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. We include a copy of the GPL with every CD shipped with our product. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. NOTA that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act

of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute

the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance

on consistent application of that system; it is up to the author/ donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

For Turkey only

Authorised distributors in Turkey:

BOGAZICI BIL GISAYAR SAN. VE TIC. A.S.
Tel. No.: +90 212 3311000
Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10 AYAZAGA/ISTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.
Tel. No.: +90 212 3567070
Address: CEMAL SURURI CD. HALIM MERIC IS MERKEZI No: 15/C D:5-6 34394 MECIDIYEKOY/ISTANBUL

KOYUNCU ELEKTRONiK BiLGi iSLEM SiST. SAN. VE DIS TIC. A.S.
Tel. No.: +90 216 5288888
Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZi, SANCAKTEPE ISTANBUL

AEEE Yönetmeliğine Uygundur.

Información de contacto con ASUS

ASUSTeK COMPUTER INC. (Asia Pacífico)

Domicilio de la compañía	15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Dirección web	www.asus.com.tw

Asistencia técnica

General (tel)	+886228943447
Asistencia (fax)	+886228907698
Asistencia en línea	support.asus.com

ASUS COMPUTER INTERNATIONAL (América)

Domicilio de la compañía	800 Corporate Way, Fremont, CA 94539, USA
General (tel)	+15107393777
General (fax)	+15106084555
Dirección web	usa.asus.com
Asistencia en línea	support.asus.com

ASUS COMPUTER GmbH (Alemania y Austria)

Domicilio de la compañía	Harkort Str. 21-23, D40880 Ratingen, Germany
General (fax)	+492102959911
Dirección web	www.asus.de
Contacto en línea	eu-rma.asus.com/sales

Asistencia técnica

Teléfono de componentes	+49-2102-5789555
Teléfono de sistemas(Alemania) /portátiles/Eee/pantallas LCD	+49-2102-5789557
Teléfono de sistemas(Austria) /portátiles/Eee/pantallas LCD	+43-820-240513
Asistencia (fax)	+49-2102-9599-11
Asistencia en línea	support.asus.com

Información telefónica internacional acerca de redes

Region	Country	Hotline Number	Service Hours
Europe	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri
	France	0033-170949400	09:00-18:00 Mon-Fri
	Germany	0049-1805010920 0049-1805010923 (component support) 0049-2102959911 (Fax)	09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
	Hungary	0036-15054561	09:00-17:30 Mon-Fri
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Austria	0043-820240513	09:00-18:00 Mon-Fri
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri
	Belgium	0032-78150231	09:00-17:00 Mon-Fri
	Norway	0047-2316-2682	09:00-18:00 Mon-Fri
	Sweden	0046-858769407	09:00-18:00 Mon-Fri
	Finland	00358-969379690	10:00-19:00 Mon-Fri
	Denmark	0045-38322943	09:00-18:00 Mon-Fri
	Poland	0048-225718040	08:30-17:30 Mon-Fri
	Spain	0034-902889688	09:00-18:00 Mon-Fri
	Portugal	00351-707500310	09:00-18:00 Mon-Fri
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri
	Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri
	Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri
	Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri
	United Kingdom	0044-8448008340	09:00-17:00 Mon-Fri
	Ireland	0035-31890719918	09:00-17:00 Mon-Fri
	Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri
	Ukraine	0038-0445457727	09:00-18:00 Mon-Fri

Información telefónica internacional acerca de redes

Region	Country	Hotline Numbers	Service Hours
Asia-Pacific	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
		0081-473905630 (Non-Toll Free)	09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717 1800-8525201	09:00-18:00 Mon-Fri
	Singapore	0065-64157917 0065-67203835 (Repair Status Only)	11:00-19:00 Mon-Fri 11:00-19:00 Mon-Fri 11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India India(WL/NW)	1800-2090365	09:00-18:00 Mon-Sat 09:00-21:00 Mon-Sun
	Indonesia	0062-2129495000 500128 (Local Only)	09:30-17:00 Mon-Fri 9:30 – 12:00 Sat
	Vietnam	1900-555581	08:00-12:00 13:30-17:30 Mon-Sat
	Hong Kong	00852-35824770	10:00-19:00 Mon-Sat
Americas	USA Canada	1-812-282-2787	8:30-12:00 EST Mon-Fri 9:00-18:00 EST Sat-Sun
	Mexico	001-8008367847	08:00-20:00 CST Mon-Fri 08:00-15:00 CST Sat

Información telefónica internacional acerca de redes

Region	Country	Hotline Numbers	Service Hours
Middle East + Africa	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
	UAE	00971-42958941	09:00-18:00 Sun-Thu
	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800	08:00-17:00 Sun-Thu
		*9770/00972-35598555	08:30-17:30 Sun-Thu
Balkan Countries	Romania	0040-213301786	09:00-18:30 Mon-Fri
	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
	Bulgaria	00359-70014411	09:30-18:30 Mon-Fri
		00359-29889170	09:30-18:00 Mon-Fri
	Croatia	00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
	Slovenia	00368-59045400 00368-59045401	08:00-16:00 Mon-Fri
	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

NOTA: Para obtener más información, visite el sitio de soporte de ASUS en: **http://support.asus.com**

Fabricante:	**ASUSTeK Computer Inc.**	
	Teléfono:	+886-2-2894-3447
	Dirección:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Representante autorizado en Europa:	**ASUS Computer GmbH**	
	Dirección:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY